BACHARELADO EM SISTEMAS DE INFORMAÇÃO

DIEGO DIAS DOS SANTOS MARTINS

# AUDITORIAS DE TESTE DE INVASÃO EM REDES GLOBAIS.

Niterói, RJ
2017

DIEGO DIAS DOS SANTOS MARTINS

# AUDITORIAS DE TESTE DE INVASÃO EM REDES GLOBAIS.

Projeto de Conclusão de Curso apresentado ao Centro Universitário La Salle do Rio De Janeiro, como parte dos requisitos necessários à obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Alex Vanderlei Salgado

Coorientador: Prof. Dr.ª Márcia de Freitas

Niterói, RJ
Outubro de 2017

**CENTRO UNIVERSITÁRIO LA SALLE DO RIO DE JANEIRO**

CURSO DE SISTEMAS DE INFORMAÇÃO

Projeto de conclusão de Curso apresentado ao Centro Universitário La Salle, em cumprimento parcial das exigências para obtenção do grau em Bacharel em Sistemas de Informação.

**Aluno**: Diego Dias dos Santos Martins

**Título do Projeto**: Auditorias de teste de invasão em redes globais.

Projeto aprovado em: _____/______/______

BANCA EXAMINADORA

_______________________________________________

Prof. Dr. Alex Vanderlei Salgado
Orientador

_______________________________________________

Prof. Dr.ª Márcia de Freitas Siqueira Sadok Menna Barreto
Coorientador

OBSERVAÇÕES:

_______________________________________________

_______________________________________________

_______________________________________________

_______________________________________________

# AUDITORIAS DE TESTE DE INVASÃO EM REDES GLOBAIS.


## RESUMO

A cibersegurança é uma área essencial para as empresas e órgãos do governo, pois ajuda a proteger as informações confidenciais contra os c*rackers* que tem como objetivo danificarem e/ou roubarem informações que sejam relevantes, para depois pedirem recompensas, como por exemplo, criptomoedas *Bitcoins.*

Diante disso, este projeto tem como objetivo verificar maneiras de descobrir falhas nos sistemas operacionais, falhas em sistemas *Webs* ou falhas humanas, e um material de estudo para cibersegurança, inclusive desvendar possíveis caminhos em que os *crackers* percorrem para saberem de informações confidenciais de empresas. Dentro do projeto será demonstrado a construção de um sistema que serve para coletar dados geográficos de servidores através de protocolos de internet. Vale ressaltar que o projeto pretende criar maneiras de proteger as informações que circulam nas redes através da internet. E por fim, será demonstrado os resultados obtidos através do *Google Earth*, além das metodologias e princípios, utilizadas para construção do sistema e do projeto.



**Palavra-chave:** Kali Linux; Linguagem Programação Perl; Hacker; Redes; Google Hacking; Cibersegurança.



## RÉSUMÉ

Cyber Security est un domaine essentiel pour les entreprises et agences gouvernementales, car elle aide à protéger les informations confidentielles contre les biscuits qui corrompu et/ou de voler des informations pertinentes, puis demandent des récompenses, comme par exemple, Criptomoedas de Bitcoins.

Par conséquent, ce projet vise à vérifier les façons de découvrir les failles dans les systèmes d'exploitation, défaillances de systèmes Web ou erreur humaine et un matériel d'étude pour la cybersécurité, y compris les chemins possibles découvrant dans les biscuits voyagent pour connaître informations confidentielles des entreprises. Dans le cadre du projet sera montré la construction d'un système qui sert à recueillir des données géographiques aux serveurs via des protocoles internet. Il est à noter que le projet a l'intention de créer des moyens de protéger les informations qui circulent dans les réseaux via internet. Et enfin, vous verrez s'afficher les résultats obtenus par l'intermédiaire de Google Earth, outre les méthodes et les principes utilisés pour la conception et la construction du système.



**Mot-clé:** Kali Linux, langage Perl, Hacker, Réseaux, Google Hacking, Cyber-sécurité.

FICHA CATALOGRÁFICA
Dias, Diego dos Santos Martins
Auditorias de teste de invasão em redes globais.
Diego Dias dos Santos Martins. Niterói: UNILASALLE-RJ, 2017. 74p.il. color. f 31 cm
Orientador: Prof. Dr. Alex Vanderlei Salgado
Coorientador: Prof. Dr. Márcia de Freitas Siqueira Sadok Menna Barreto
Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) – UNILASALLE-RJ – Centro Universitário La Salle-RJ.
Referências: f. 69
1. defesa, hackers, rede, invasão 2. SALGADO, Alex Vanderlei, 3. Centro Universitário La Salle do Rio de Janeiro, 4. Auditorias de teste de invasão em redes globais.

## Sumário

## 1. INTRODUÇÃO

Após os múltiplos ciberataques de 12 de maio de 2017, em quase todos os países, logo se levantou a discussão sobre os *crackers* como forma proeminente de segurança, uma vez que, o ciberataques surge como oportunidade dos *crackers* de causar danos em proporções ainda não vivenciadas.

Os *crackers* representa uma ameaça real devido ao rápido desenvolvimento tecnológico, onde os alvos potenciais são os sistemas que controlam as defesas e infraestruturas críticas das nações. O rápido crescimento dos usuários, bem como a dependência da Internet aumentaram drasticamente os riscos de segurança, ao menos que haja medidas de segurança adequadas para ajudar na prevenção, danos severos ou outras consequências sociais, ideológicas, religiosas e políticas poderão ser causados através do acesso de redes em sistemas de informações em locais mais remotos do planeta.

Outra questão relevante, diz respeito à disposição em fazer parte de um grupo de *crackers*. Incialmente é um dos métodos mais baratos de *crackers*, pois necessita na maioria das vezes apenas de um computador pessoal, e de um vírus *Ransomware* e uma conexão on-line. A dificuldade em rastrear a identidade real dos invasores facilita o anonimato e a quantidade de objetos-alvos é bastante variável.

Estudos demostram que as infraestruturas críticas, como as redes de energia elétrica e os serviços essenciais, são vulneráveis a ataques *crackers* porque os sistemas de informação que os executam são altamente complexos, tornando-os eficazes para ataques devido à impossibilidade de eliminar todas as fraquezas.

Desta forma é necessário que instituições governamentais e empresas de segurança de todo o mundo, se unam e tentem harmonizar as ações que constituem atividades criminosas no domínio cibernético para capacitar as agências de inteligência e empresas de segurança com tecnologia de segurança com intenção de investigar tais atividades e impedir tais ataques antes que causem consequências potencialmente danosas a sociedade global.

# 2. OBJETIVOS

## 2.1. Objetivo Geral

É dentro deste contexto, que o presente estudo tem como objetivo:

Elaborar um sistema que demonstre a informações da localização de endereços de protocolos *internet* atribuídos a empresas em vários países.

## 2.2. Objetivos Específicos

A fim de fomentar a proteção da informação:

1) Mostrar a importância da segurança e a defesa cibernética.

2) Ampliar a percepção dos riscos associados a novas ferramentas e meios de violação desenvolvidos por Crackers para interceptarem os dados;

3) Garantir a estabilidade e integridade dos sistemas e;

4) Resguardar e preservar a confidencialidade das informações.

# 3. JUSTIFICATIVA

Nos dias atuais devido aos avanços tecnológicos e a globalização, cada vez mais a internet tem sido utilizada como meio para solucionar tarefas cotidianas. Um indivíduo pode acessar suas informações em qualquer parte, seja a mais remota do mundo. Assim, constantemente, dados como senhas de e-mails, contas bancárias, número de cartão previdenciário e crédito, estão trafegando pela rede entre um computador e outro.

Muitos são os dispositivos utilizados, como a exemplo os *firewalls*, antivírus e *antispyware* para tornarem a navegação digital mais segura, porém, infelizmente, os *crackers* também se adaptaram aos avanços da tecnologia e, assim, pessoas, organizações públicas e privadas estão se tornando, habitualmente, vítimas de violações cometidas através da Internet.

Em seu livro "A internet e os *Hackers* Ataques e Defesas" (2000), Márcio José, expõe que grande parte dos ataques *crackers* tem como objetivos colocar seus sistemas em tela azul parando totalmente o funcionamento do mouse para comandos.

Durante a apresentação do relatório anual de 2016, pela Organização do Tratado do Atlântico Norte (OTAN), o secretário-geral Jens Stoltenberg afirma que a instituição

apresentou um aumento de 60% em relação a 2015, no número de ataques cibernéticos (EL PAÍS; 2017).

O Brasil tornou-se grande alvo de *crackers*, principalmente na esfera cibernética. Calcula-se que os Jogos Olímpicos de Londres, em 2012, tenham sofrido pelo menos 97 incidentes graves de segurança, envolvendo, principalmente, ataques de negação de serviço (DDoS). Diante disso, será preciso analisar a segurança em ciberespaços, pois estes são vitais para o recrutamento de c*rackers*, bem como, para proteger principalmente os sistemas de controle de infraestrutura crítica, como a exemplo a rede de distribuição de energia e aeroportos, com o propósito de evitar danos ou interrupções sérias, levando risco à sociedade (ALCÂNTARA, 2015; DATASUS; 2016).

## 4. HIPÓTESE

Há necessidade de assegurar a confiabilidade, a integridade das informações e a disponibilidade da comunicação, intensificando a identificação de vulnerabilidades nas estruturas de segurança da informação, a fim de aperfeiçoar a infraestrutura de proteção e minimizar os danos causados pelos *crackers*.

## 5. REFERENCIAL TEÓRICO

### 5.1. Atuação da perícia forense computacional.

Os ataques cibernéticos podem envolver uma quantidade muito ampla de métodos, que requerem procedimentos diferentes para melhorar a segurança computacional. Haja vista a eliminação de fronteiras oferecida pela Internet, sérias dificuldades acabaram-se desenvolvendo para combater esses tipos de delitos, tornando-se mais fácil sua prática e ocorrência onde vítimas e criminosos podem estar em países distintos e também distantes (FRANCO, 2016).

Neste contexto, surge a necessidade de uma área especializada com amplo conhecimento em computação, a segurança da informação, o direito digital e outras áreas afins, com capacidade suficiente para investigar quem, como e quando um crime cibernético foi praticado, assim surge a perícia forense computacional (FRANCO, 2016).

De acordo com o dicionário Aurélio de Língua Portuguesa, a palavra forense significa

“que se refere a foro judicial” e a palavra perícia significa “sabedoria, prática, experiência, habilidade em alguma ciência ou arte”. Desta maneira, a perícia forense computacional é a união entre os conhecimentos da área da informática e da área jurídica, que por meio de métodos técnico-científicos, tem como objetivo coletar evidências digitais, analisar dados e apresentar provas perante um ambiente jurídico, visando sempre proteger usuários e recursos da exploração, invasão de privacidade na forma digital e/ou qualquer outro crime (DE SOUZA; 2015; SOUZA; 2016).

Para a execução da perícia forense, Kent et. Al (2006) sugere uma sequência de procedimentos forense, que podem ser ajustados com o decorrer da perícia. A sequência é formada por quatro etapas (Figura 1):

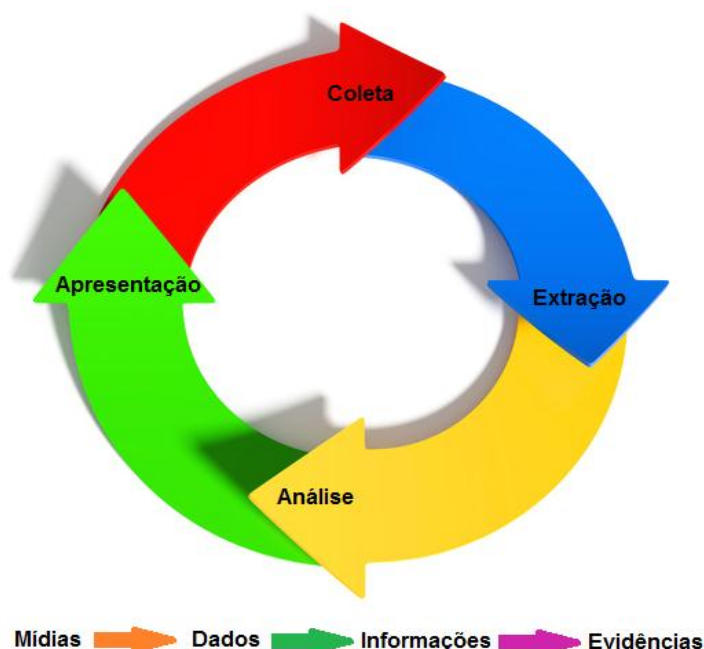



Figura 1: Etapas do processo forense
Fonte: Adaptado de KENT; et al. (2006).

- **Coleta**: é executada a identificação de elementos que provavelmente contenham evidências digitais ou que possuam alguma relação com o incidente que está sendo investigado;

- **Extração**: identificar, recuperar e extrair as informações relevantes a partir dos dados coletados utilizando ferramentas e técnicas forenses que sejam pertinentes à investigação;

- **Análise**: analisar os dados/informações do exame para elaborar respostas úteis para as questões apresentadas nas fases anteriores.

- **Apresentação**: tem como finalidade documentar as evidências digitais encontradas e apresentá-las às autoridades competentes. O laudo técnico pericial deve ser conciso, de fácil leitura, descrevendo de forma objetiva e clara os métodos, ferramentas e exames realizados durante o processo forense.

### 5.2. Espaço cibernético para práticas ilegais.

A sociedade moderna é marcada por um cenário em transformação pelo uso de alta tecnologia, introduzindo uma nova dimensão as formas de comunicação. A internet é uma realidade global que significa um grande marco para as comunicações. Manuel Castells (2003) afirma que a Internet constitui a base material e tecnológica da sociedade em rede, não sendo simplesmente uma tecnologia, mas um meio de comunicação que permite, pela primeira vez, a comunicação de muitos com muitos, num momento escolhido, em escala global, sem fronteiras para restringir sua utilização.

O espaço físico e virtual passa a conviver com a complexidade da configuração cibernética. Neste sentido, surge o conceito de espaço cibernético, novo espaço onde ocorrem as relações humanas de grande importante, nas esferas políticas, econômicas, científicas e sociais. O espaço cibernético é "*a instauração de uma rede de todas as memórias informatizadas e de todos os computadores*" (LÉVY, 2007).

Com o avanço da tecnologia computacional e a da instauração de uma rede com todas as memórias informatizadas é importante compreender a ética da informática relacionada à segurança. Algumas perguntas necessitam ser abordadas quanto às questões éticas globais, tais como: - Quais informações sobre o indivíduo podem ser reveladas a outras pessoas? - Quais informações individuais devem ser mantidas em bancos de dados, e quão seguras são os sistemas de computador? - Como lidar com a pirataria de dados nas redes de computadores? - Como garantir que as informações sejam salvaguardas e só possam ser acessadas por pessoas e organizações autorizadas? (GUNARTO, 2017).

Neste contexto, com o crescimento de ferramentas gratuitas que são utilizadas para formular ataques, as poucas leis de prevenção de crimes digitais e o crescente número de grupos organizados que exploram as deficiências de segurança, veem se apontando as oportunidades para o cibercrimes (ÂNGELO, 2002).

Entende-se por cibercrimes ou crime virtual qualquer ação que infringem as normas éticas uma vez que esses prejudicam a sociedade em geral, onde o computador seja o instrumento ou objeto do delito, ou então, qualquer delito ligado ao tratamento automático de dados (VAREJÃO, 2004).

Com a investigação dos cibercrimes, surgiu à necessidade de caracterizar um perfil dos grupos que cometem esses crimes, assim surgiu o personagem *"hacker"*. Segundo tradução do dicionário Michaelis o termo *hacker*, quer dizer "*indivíduo que se dedica a entender o funcionamento interno de dispositivos, programas e redes de informática com o fim, entre outras coisas, de encontrar falhas em sua segurança ou conseguir um atalho inteligente que possa vir a resultar em um novo recurso ou ferramenta*". Porém, como têm sido divulgados por muito tempo através das mídias mundiais, os *hackers* são denominados indivíduos que invadem os sistemas de segurança e quebram os códigos computacionais para fins ilegais como, por exemplo, fraudar sistema telefônico, copiar programa de computador ou material audiovisual, fonográfico etc., sem autorização do autor ou sem respeito aos direitos de autoria e cópia, para comercialização ou uso pessoal. Assim, os *hackers* criaram a termo "*cracker*", oriundo de *Criminal Hacker*, para nomear estes tipos de criminosos que em geral, são repudiados pelos membros das comunidades internacionais de software livre (AGUIAR, ET AL., 2009).

Desta maneira, o vasto conhecimento aprofundado em tecnologia de sistemas entre *hackers* e os *crackers* geralmente são muito parecidos, porém, a principal diferença é a finalidade do uso deste conhecimento e as práticas resultantes. Enquanto os *crackers* são motivados por objetivos criminosos de obter vantagens de formas ilícitas, os *hackers* realizam atividades positivas, de desenvolvimento e aperfeiçoamento. Assim, por onde os *crackers* percorrem os *hackers* seguem seus passos para evitar que os problemas causem maiores danos.

Com a evolução da tecnologia, as ameaças cibernéticas podem ser executadas de diferentes formas, o que diferenciará o tipo de ataque dependerá do objeto-alvo e da motivação, sendo os tipos de ameaças agrupadas em (IDN; 2013):

- **Cibercrime**: Essencialmente de característica de benefício econômico próprio através de ações ilegais, como fraudes bancárias, roubo de número de cartão de crédito e transações financeiras.

- **Ciberespionagem**: O foco principal é obtenção de informações importantes, seja de organizações governamentais ou privadas, para obtenção de benefício próprio ou posterior venda.

### 5.3. Criptomoeda *Bitcoin*

O *Bitcoin* é uma criptomoeda descentralizada apresentada em 2008 durante o grupo de discussão *The Cryptography Mailing* por um programador ou grupo de programadores, de pseudônimo "*Satoshi Nakamoto*". Em 2009, torna-se também um sistema ou rede de pagamento online baseado em protocolo de código aberto independente chamado do "sistema eletrônico de pagamento *peer-to-peer*" (P2P ou ponto-a-ponto). Como o *Bitcoin* e o *Ethereum* e outros criptomoedas são utilizadas pelos hackers e crackers como forma para pagar e solicitar pagamento de usuários e empresas, elas têm proteções de segurança e algumas são impossíveis de rastrear como por exemplo o *Ethereum*, já diferente do *Bitcoin* que é possível saber quem está recebendo o dinheiro e quem pagou, no entanto é necessário saber muito da tecnologia.

Figura 2: Criptomoeda Bitcoin.
Fonte: Infoeuropefx.com, 2017.

### 5.4. Descrição de códigos maliciosos.

De acordo com a cartilha do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT, 2017), os códigos maliciosos (*malwares*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- Pela exploração de vulnerabilidades existentes nos programas instalados.

- Pelo auto execução de mídias removíveis infectadas, como *pen-drives*.
- Pelo acesso a páginas *web* maliciosas, utilizando navegadores vulneráveis;

Figura 3: *Malwares*.
Fonte: CERT, 2017.

De acordo com cartilha do CERT (2017), os principais motivos que levam um atacante a desenvolver e propagar códigos maliciosos são a obtenção de vantagens financeiras, e coleta de informações confidenciais e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários que possibilitam a prática de golpes, a realização de ataques e a disseminação de *spam*.

### 5.5. A internet em computadores.

A rede computadores é formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema de comunicação, ou seja, é quando há pelo menos dois ou mais computadores, e outros dispositivos interligados entre si de tal modo que podem compartilhar recursos físicos e lógicos, estes podendo ser do tipo: dados, impressoras, mensagens (e-mails), dentre outros (MENDES, 2007).

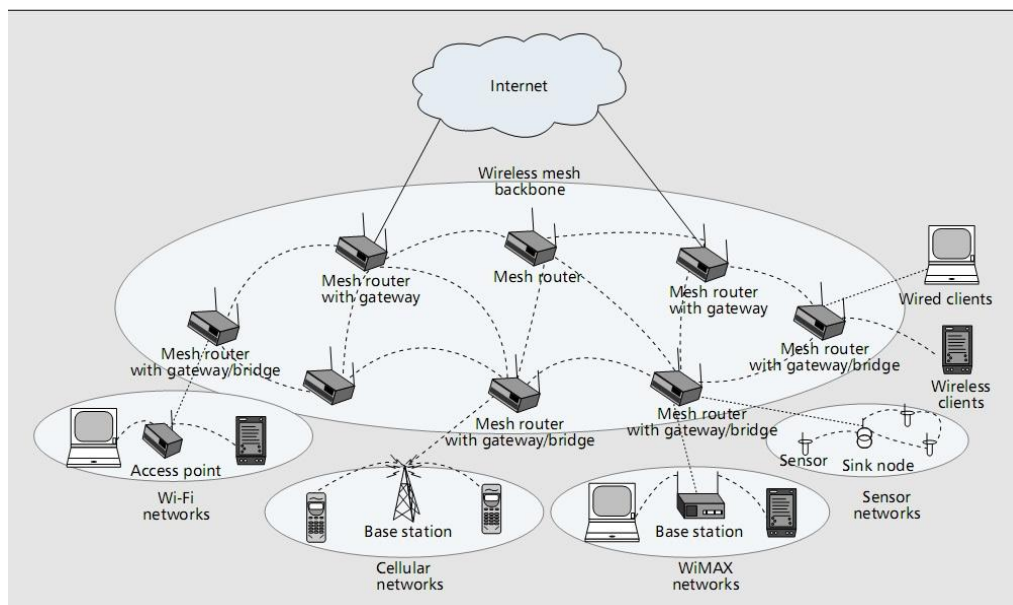



Figura 4: Redes de computadores.
Fonte: Redes sem fio em malha, 2017.

### 5.6. A internet em computadores.

Conforme o Mendes (2007), a Internet é um sistema global de redes de computadores que ao serem interligados utilizam um conjunto próprio de protocolos (*Internet Protocol Suite* ou TCP/IP), que tem como finalidade servir progressivamente usuários no mundo inteiro. A internet apresenta uma diversidade de recursos de informação e serviços, tais como os documentos inter-relacionados de hipertextos da *World Wide Web* (WWW), redes ponto-a-ponto (*peer-to-peer*) e infraestrutura de apoio a correio eletrônico (e-mails). O desenvolvimento da *World Wide Web* começou no final da década de 1980, quando um grupo de investigadores do CERN (*Centre Européen por la Recherche Nucléaire*) iniciou o desenvolvimento de um sistema que permitisse partilhar documentos científicos. O engenheiro Tim Berners-Lee, desenvolveram o ENQUIRE, projeto usado para reconhecer e armazenar associações de informações. Cada nova página no ENQUIRE deveria estar ligada a uma página existente.

### 5.7. Uso de Sistemas de Informações Geográficas.

Pretendendo localizar cada ponto da superfície do globo terrestre, fora criado um sistema de linhas imaginárias intitulado de Sistema de Coordenadas Geográficas. A coordenada geográfica de um ponto específico da superfície do planeta é resultante da interseção de um meridiano e um paralelo (RECESA, 2013).

Os Meridianos são linhas imaginárias que cortam a Terra no sentido Norte-Sul,

ligando um polo ao outro. O meridiano central (Greenwich) divide a Terra em dois hemisférios e a sua gradação vai até 180º tanto para Leste (E) quanto para Oeste (W). Os paralelos são círculos da esfera cujo plano é perpendicular ao eixo dos polos. O equador é o paralelo que divide a Terra em dois hemisférios (Norte e Sul). A linha do Equador corresponde ao paralelo de origem (0º), seguindo a 90º em direção aos polos, indicando a posição no hemisfério Sul (S) ou no hemisfério Norte (N) (TERRAVIEW; 2011; RECESA; 2013).

Assim, as coordenadas geográficas que definem um ponto específico na Terra correspondem ao conjunto de latitudes e longitudes. Onde longitude é o valor angular do arco compreendido entre o meridiano de Greenwich (0º) e o lugar de referência que varia entre 0° a ±180° (W/E) e latitude é o valor angular do arco compreendido entre o equador e o lugar de referência que varia de 0° a ±90° (N/S) (MARQUES; 2017).

A partir da metade do século XX, por meio do uso da informática, possibilitou-se fazer análises criteriosas de projeção cartográfica combinando diferentes mapas e dados, uma vez que há uma variedade de modos de projetar sobre um plano os objetos geográficos que caracterizam a superfície terrestre, dando origem ao geoprocessamento (TERRAVIEW; 2011).

Segundo Câmara e Davis (2001) geoprocessamento denota a disciplina do conhecimento que utiliza técnicas matemáticas e computacionais para o tratamento da informação geográfica. Moreira, et. al. (2011), complementa que o geoprocessamento pode tratar dados de objetos ou fenômenos geograficamente identificados ou extrair informações desses objetos ou fenômenos, quando eles são observados por um sistema sensor.

Desta maneira o geoprocessamento tem sido amplamente empregado na Cartografia, Análise Ambiental, Transporte, Energia, Planejamento Urbano, Saúde e mais recentemente na Segurança Pública. Para cada uma dessas áreas é necessário um sistema específico. As ferramentas computacionais para executar o geoprocessamento são chamadas de Sistemas de Informação Geográfica (SIG ou (inglês) – *Geographic Information Systems*), que permite realizar análises complexas, ao integrar dados de diversas fontes e criar bancos de dados georreferenciados (NICOLAU; 2005).

Teixeira et al. (1995), define SIG como um conjunto de programas, equipamentos, metodologias, dados e pessoas (usuários), perfeitamente integrados, de forma a tornar possível a coleta, o armazenamento, o processamento e a análise de aplicação. O SIG visa

propor maior facilidade, segurança e agilidade nas atividades humanas referentes ao monitoramento, planejamento e tomada de decisão relativa ao espaço geográfico.

Um SIG, possui a seguinte estrutura (CÂMARA; DAVIS; 2001):

- Interface com usuário;

- Entrada e integração de dados;

- Funções de processamento gráfico e de imagens;

- Visualização e plotagem;

- Armazenamento e recuperação de dados (organizados sob a forma de um banco de dados geográficos).

Estes componentes fundamentais que configuram um SIG, devem funcionar em plena harmonia e integração para que o sistema funcione satisfatoriamente (Figura 5).

Figura 7: Componentes de um SIG.
Fonte: Geoinformática, 2012.

Os dados agora georreferenciados podem ser utilizados nas mais variadas aplicações, tornando-se uma poderosa ferramenta no auxílio à tomada de decisões, pesquisas, entre outros, como, por exemplo: aquelas que envolvem o uso da terra, seres humanos e a infraestrutura existente; aplicações ambientais, enfocando o meio ambiente e o uso de recursos naturais; aplicações de gerenciamento, de como alocar recursos para remediar problemas ou garantir a preservação de determinadas características; e de modo mais recente

para análises criminais (NICOLAU, 2005).

Há uma crescente mudança dos crimes no século XXI, que se expandiu para os ciberespaços, dentre eles o Ciberataques. O ciberespaço é uma ameaça real e no futuro, será pelo menos tão perigoso quanto o campo de batalha físico. Assim, as tecnologias geoespaciais estão sendo adaptadas combinando tecnologias de vigilância, dados e SIG, bem como as práticas de monitoramento, identificação e captura com o objetivo de proteger as informações empresariais e governamentais contra os ataques de crackers. (LATTIMER, 2013).

## 5.8. Estratégias de segurança ofensiva de redes cibernéticas.

O avanço das chamadas tecnologias de informação e comunicação (TICs) trouxeram grandes benefícios, no entanto, fizeram surgir um dos maiores desafios do novo século em termos de segurança, os ataques cibernéticos.

Segundo o Departamento de Segurança Interna dos Estados Unidos, a segurança cibernética inclui a vigilância aos danos causados pelo uso não autorizado da informação eletrônica e de sistemas de comunicações e a respectiva informação neles contida, tendo em vista preservar a confidencialidade, integridade e disponibilidade, incluindo ainda ações para restabelecer a informação eletrônica e os sistemas de comunicações no caso de um ataque *crackers* ou de um desastre natural (NIPP; 2009).

Com o acelerado ritmo de competitividade do mercado em lançar novos produtos tecnológicos, dentre *hardware* e *software*, sem que estejam completamente testados, gerando equipamentos com potenciais problemas de funcionamento assim, cria-se uma nova vulnerabilidade estrutural e funcional das redes e também dos sistemas que unificam as infraestruturas de informação (IDN, 2013).

Outro fator relevante, de grande preocupação refere-se à dependência do pleno funcionamento das redes de telecomunicações para a operação de infraestruturas críticas como as centrais de produção e distribuição de energia elétrica, os serviços de emergência, o sistema bancário e os próprios sistemas de comando e controle das Forças Armadas.

Diante do risco presente, a segurança e a proteção contínua das infraestruturas de informação têm de ser vista como um processo contínuo e sistêmico. Desta maneira, empresas e organizações voltadas para o desenvolvimento de tecnologias de informação, constituem um

mecanismo destinado a desvendar vulnerabilidades que provoquem erros em seus produtos.

Em função da sensibilidade das informações é necessário estabelecer uma estratégia ofensiva, ou seja, uma abordagem proativa e hostil para proteger, sistemas, redes e indivíduos de ataques. A segurança convencional, por vezes referida como "segurança defensiva", centra-se em medidas conservadoras, tais como correção de *software*, encontrar e corrigir vulnerabilidades do sistema. Em contraste, as medidas de segurança ofensivas estão focadas na busca dos invasores e em alguns casos tentar desativar, interromper ou pelo menos minimizar os impactos de suas operações.

Na era da informação, ao que diz respeito ao âmbito militar, o próprio ciberespaço é utilizado para conduzir todo o conjunto das operações, dando origem ao conceito de Operações no Ciberespaço, ou *Computer Network Operations* (CNO), cujo Departamento de Defesa dos Estados Unidos (DoD – *United States Department of Defense*) instrui que o CNO para explorar possíveis capacidades dos adversários deve ser composto de:

- ***Computer Network Defense*** (CND): Medidas defensivas para proteger e defender informações, computadores e redes de ataques de interrupção, negação, degradação ou destruição.
- ***Computer Network Exploitation*** (CNE): Técnica onde redes de computadores são utilizadas para infiltrar outras redes de computadores alvo para extrair e recolher dados de inteligência. Permite a exploração de computadores individuais e redes de computadores de uma organização ou país externo, a fim de recolher dados vulneráveis ou confidenciais, que normalmente são mantidos ocultos e protegidos do público em geral.
- ***Computer Network Attack*** (CNA): Operações para interromper, negar, degradar, ou destruir informações nas redes de comunicação de possíveis adversários ou em computadores, redes e sistemas próprios.

Diante da crescente habilidade em interromper e destruir os sistemas de informação e telecomunicações. A OTAN e a UE tem unido esforços junto aos EUA, diante das ameaças globais atribuídas aos ciberespaços (IDN, 2013).

# 6. PROCEDIMENTOS METODOLÓGICOS

## 6.1. Passos propostos para a execução do trabalho.

1) Escolha do tema:

De acordo com alguns estudos, os *crackers* fazem uso das tecnologias de telecomunicação para invadir órgãos governamentais, empresas privadas, com objetivo de solicitarem recompensas pelo mundo para liberar os dados dos sistemas das vítimas. Saber o conhecimento e informação da localização das empresas e órgãos governamentais, tarefa sugerida por este projeto demonstra sua importância no contexto de Segurança Pública mundial.

2) Pesquisa de referências bibliográficas nacionais e internacionais sobre o assunto abordado:

Através de pesquisas à Internet em sites e repositores de publicações científicas de Universidades nacionais e internacionais pôde-se obter um conjunto significativo de bibliografias e informações sobre o assunto abordado.

3) Etapas para o desempenho do software *Information*:

a. **Coleta**: A equipe de *hackers* éticos irão usar técnicas forense computacional para busca na Internet por pessoas, empresas e órgão dos governos. As evidências forenses irão mostra falhas de segurança dos sites e das empresas como todo; a coleta de dados das usuários e empresas serão realizados nos ambientes *surface web* (partes indexadas) e ambientes *deep web* (não-indexados) utilizando como ferramenta o buscador Google, com uso de navegadores convencionais como Chrome, Mozilla Firefox, Internet Explorer e o buscador DuckDuckGo que utilizam as ferramentas intermediárias *Tor* ou *Tor2web*. Além disso, irão usar técnicas de Engenharia social para obter dados e informações, explorando as fraquezas humanas inerentes a toda organização.

b.**Extração**: As informações geográficas dos usuários e empresas serão fornecidas pelo sistema *Information* a partir da inserção de um IP ou de uma URL.

c. **Funcionamento do *software***: O *Information* será construído em linguagem programação Perl, utilizando biblioteca do módulo *Comprehensive Perl Archive Network* (CPAN) que possui ferramentas que irão garantir a qualidade do software. O *Information* obterá dados de provedores de internet e endereços de site através da integração com o

sistema API-IP. Este sistema irá consultar o mecanismo de *layout* Gecko que foi desenhado para suportar os padrões abertos da Internet como HTML, Javascript, DOM, XML, dentre outros. Com o objetivo de obter dados, o Gecko se interligará ao GetKong que também é um intermediador entre sistemas e de bancos de dados geográficos. Ao final esses dados retornarão sistema API-IP e para o sistema *Information* a fim de gerar informações.

d. **Análise**: Como posse dos dados obtidos pelo sistema *Information* mostrará como os sistemas são vulneráveis e como é acessível obter informação de usuários e empresas.

e. **Apresentação**: Serão demonstrados informações em forma de mapas para facilitar o entendimento da localização dos computadores. Estes mapas serão disponibilizados através dos serviços do sistema *Google Earth* que ilustra o mapeamento da informação geográfica.

### 6.2. Diagrama de mapa mental.

Desenvolvida pelo inglês Tony Buzan, em Londres, na última década de 70, a técnica de construção de mapas mentais, sendo um diagrama sistematizado, voltado para a gestão de informações, de conhecimento e de capital intelectual; para a compreensão a solução de problemas, fazendo uso de estratégias de trabalho e de anotações diferenciadas, com cores, desenhos, símbolos e ilustrações, para a compreensão a solução de problemas; na memorização e aprendizado, auxiliando na criação de manuais, livros e palestras; como ferramentas de brainstorming (tempestade de ideias); e no auxílio da gestão estratégica de uma empresa ou negócio (DEBASTIANI, 2015). O mapa mental (figura 8) foi construído no software  Coggle.

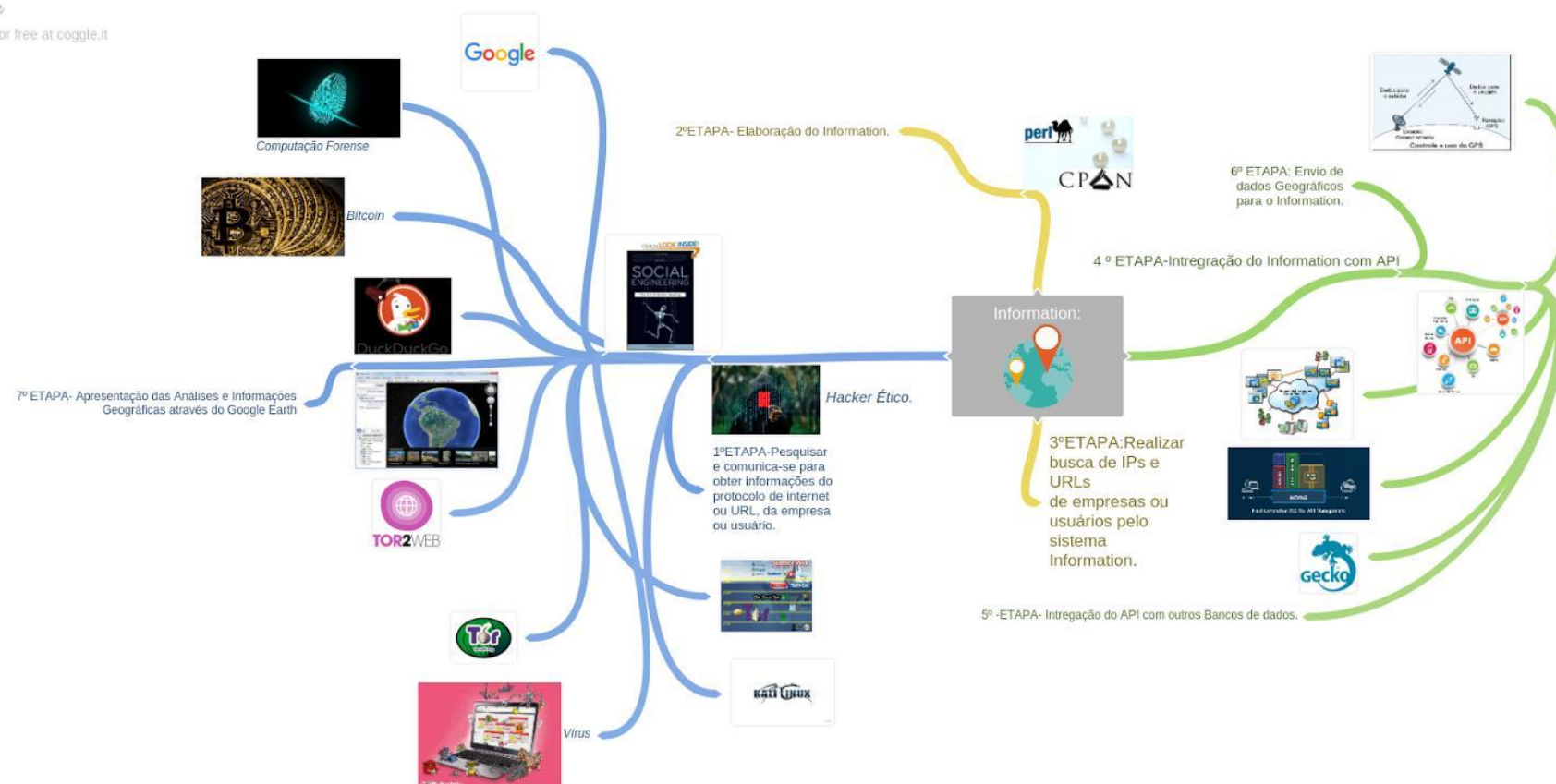



Figura 8: Mapa mental do funcionamento do sistema *Information.*
Fonte: Próprio autor.

### 6.3. O sistema operacional Kali Linux.

De acordo com a empresa *Offensive Security*, primeira etapa que um *hacker* ético deve fazer é selecionar as suas ferramentas para teste de invasão. E para este trabalho foi escolhido o *Kali Linux*, pois possui um conjunto de *softwares* desde recolhimento de informação até teste de invasão.

A equipe certificadora *Offensive Security* define que Kali Linux como uma distribuição Linux baseada em Debian destinada a testes de penetração e auditoria de segurança. O Kali Linux contém várias ferramentas, voltadas para várias tarefas de segurança da informação, como teste de penetração, pesquisa de segurança, computação forense e engenharia reversa. Lembrando que Kali Linux é desenvolvido, financiado e mantido pela *Offensive Security*, uma empresa líder em treinamento de segurança de informações (LINUX DESCOMPLICADO, 2017).

O Kali Linux foi lançado em 2013 como uma reconstrução completa, de cima para baixo, do BackTrack Linux, aderindo completamente aos padrões de desenvolvimento da Debian. Este, sistema é especificamente adaptado às necessidades dos profissionais de testes de penetração.

### 6.4. A metodologias e relatórios.

Em seu livro Introdução ao Hacking e aos Testes de Invasão , Patrick Engebretson (2014) ele fala que existe uma metodologia a seguir, como ocorre em quase tudo. O processo geral para realizar o teste de invasão pode ser dividido em uma série de passos ou de fases, quando reunidos, esses passos constituem um procedimento abrangente para realizar um teste de invasão. A análise deve ocorrer em relatórios não confidenciais sobre repostas a incidentes ou revelações sobre violação de dados dando suporte à ideia de que a maioria dos *hackers black hat* (*crackers*) também seguem um processo quando eles pretendem atacar um alvo. Usar uma abordagem organizada é importante porque não só mantém o *pentester* focado e avançando, mas também permite que os resultados ou a saída de cada passo sejam usados nos passos subsequentes (ENGEBRETSON, 2014).

A metodologia *Hacking* Entrada de Zero para teste de invasão é composta por quatro etapas que consistem em: Reconhecimento, *Scanning*, Exploração de falhas (*exploitation*) e Pós-Exploração (ou Preservação do Acesso). É importante entender que, embora a terminologia específica possa ser diferente, a maioria das metodologias robustas de testes de

invasão aborda os mesmos tópicos (ENGEBRETSON, 2014).

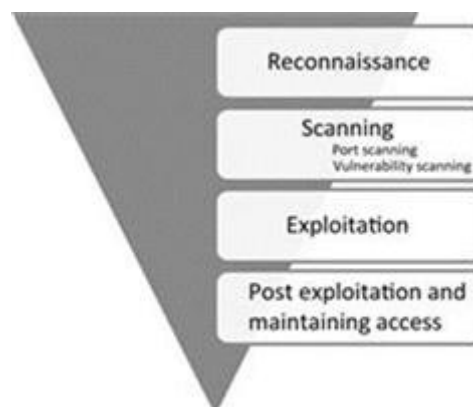
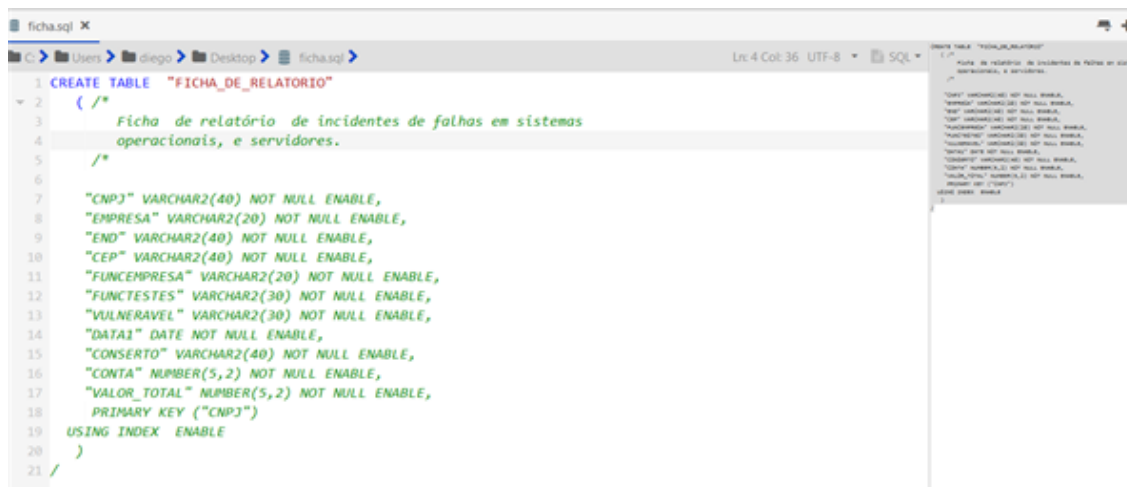



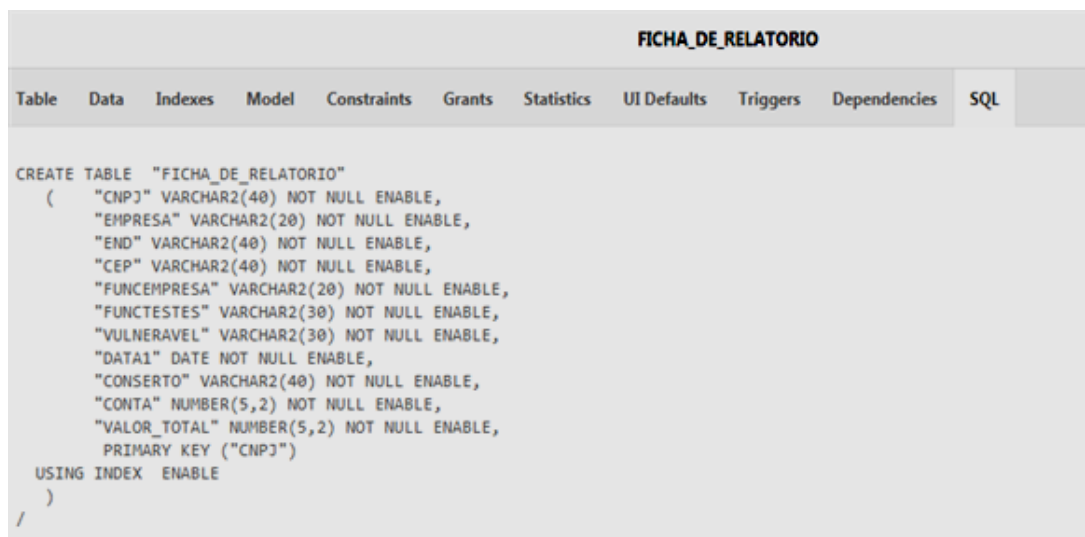
Figura 9: A metodologia *Hacking* de Entrada Zero para testes de invasão.
Fonte: Disruptive Labs, 2017.

Existem, regras estabelecidas pelo PTES (*Penetration Testing Execution Standard* ou Padrão para Execução de Testes de Invasão) é um excelente recurso de metodologia completa. O PTES inclui diretrizes técnicas que podem ser usadas por profissionais da área de segurança, além de uma *framework* e uma linguagem comum para compreensão empresarial. Mais detalhas visite o link (http://www.pentest-standard.org).

### 6.5. A metodologia ZEH.

- Reconhecimento (*Reconnaisance*): Tem como objetivo um ato de coleta de dados ou inteligência preliminares sobre seu alvo recolher o máximo de informação interessante possível. Pode ser ativamente (o que significa que você está tocando diretamente o alvo) ou passivamente (o que significa que o seu reconhecimento está sendo realizado através de um intermediário).

- Digitalização. (*Scanning*): .É scanner vulnerabilidade usado para reunir informações sobre alvo. Mais informações visite o link.(https://periciacomputacional.com/pentest-seguranca-ofensiva).

- Exploração de falhas (*Exploitation*): Corresponde ao processo de obter o controle sobre um sistema.

- Pós-exploração e preservação do acesso (*Post exploitation and maintaing access*): Consiste em permitir a preservação do acesso a um sistema remoto (ENGEBRETSON, 2014).

### 6.6. Software Oracle Apex.

De acordo com a documentação do Oracle Apex, ele é um ambiente de desenvolvimento web do Banco de Dados Oracle. Usando nada mais do que um navegador web modernos, que pode facilmente e rapidamente criar aplicativos web modernos, responsivos, seguros e escaláveis. Dentro do Oracle Apex foi criado tabela de ficha de relatório, para demonstra incidentes de sistemas dentro de uma empresa (SOUZA, 2015).

```
CREATE TABLE  "FICHA_DE_RELATORIO"
   ( /*
        Ficha  de relatório  de incidentes de falhas em sistemas
        operacionais, e servidores.
     /*

    "CNPJ" VARCHAR2(40) NOT NULL ENABLE,
    "EMPRESA" VARCHAR2(20) NOT NULL ENABLE,
    "END" VARCHAR2(40) NOT NULL ENABLE,
    "CEP" VARCHAR2(40) NOT NULL ENABLE,
    "FUNCEMPRESA" VARCHAR2(20) NOT NULL ENABLE,
    "FUNCTESTES" VARCHAR2(30) NOT NULL ENABLE,
    "VULNERAVEL" VARCHAR2(30) NOT NULL ENABLE,
    "DATA1" DATE NOT NULL ENABLE,
    "CONSERTO" VARCHAR2(40) NOT NULL ENABLE,
    "CONTA" NUMBER(5,2) NOT NULL ENABLE,
    "VALOR_TOTAL" NUMBER(5,2) NOT NULL ENABLE,
     PRIMARY KEY ("CNPJ")
  USING INDEX  ENABLE
   )
/
```

Figura 10: O código escrito em linguagem programação SQL para o sistema gerenciador de banco de dados Oracle Apex através do editor Komodo Edit 10.1.
Fonte: próprio autor.

```
CREATE TABLE  "FICHA_DE_RELATORIO"
   (    "CNPJ" VARCHAR2(40) NOT NULL ENABLE,
        "EMPRESA" VARCHAR2(20) NOT NULL ENABLE,
        "END" VARCHAR2(40) NOT NULL ENABLE,
        "CEP" VARCHAR2(40) NOT NULL ENABLE,
        "FUNCEMPRESA" VARCHAR2(20) NOT NULL ENABLE,
        "FUNCTESTES" VARCHAR2(30) NOT NULL ENABLE,
        "VULNERAVEL" VARCHAR2(30) NOT NULL ENABLE,
        "DATA1" DATE NOT NULL ENABLE,
        "CONSERTO" VARCHAR2(40) NOT NULL ENABLE,
        "CONTA" NUMBER(5,2) NOT NULL ENABLE,
        "VALOR_TOTAL" NUMBER(5,2) NOT NULL ENABLE,
         PRIMARY KEY ("CNPJ")
  USING INDEX  ENABLE
   )
/
```

Figura 11: Código de SQL dentro do Oracle Apex.
Fonte: próprio autor.

Figura 12: Relatório criado dentro do Oracle Apex descrevendo como explorar algumas falhas no sistema Windows.
Fonte próprio autor.

### 6.7. Realizando o reconhecimento de teste de Invasão.

Conforme Patrick Engebretson (2014), os primeiros passos deverá ser analisando cuidadosamente o site do alvo. Em alguns casos pode ser benéfico usar o *HTTrack* uma ferramenta conhecida por ser um utilitário gratuito que cria uma cópia *off-line* idêntica do site alvo. O site copiado inclui todas as páginas, links, figuras e o código do site original, no entanto, continuará em seu computador local. O uso de *softwares* como o *HTTrack* para cópia de sites permitirá explorar e eliminar completamente o site *off-line*, sem a necessidade de tempo adicional para vasculhar o servidor web da empresa.

O *HTTrack* foi instalado no Ubuntu de acordo com seguintes comandos abaixo. Além disso, será mostrado a tela de instalação e de resultado obtidos com *HTTrack*.

- sudo-s
- apt-get install httrack
- HTTrack www.geoespacial.com.br

```
root@diego-Aspire-ES1-511: ~
root@diego-Aspire-ES1-511:~# apt-get install httrack
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Pacotes sugeridos:
  httrack-doc
Os NOVOS pacotes a seguir serão instalados:
  httrack
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 1 não a
tualizados.
É preciso baixar 31,9 kB de arquivos.
Depois desta operação, 111 kB adicionais de espaço em disco serão usados.
Obter:1 http://br.archive.ubuntu.com/ubuntu/ precise/universe httrack i386 3.44.
1-4 [31,9 kB]
Baixados 31,9 kB em 0s (95,2 kB/s)
Selecionando pacote httrack previamente não selecionado.
(Lendo banco de dados ... 55%
```

Figura 13: Instalação do HTTrack.
Fonte: próprio autor.

```
diego-Aspire-ES1-511: ~                                        11:51  diego
diego@diego-Aspire-ES1-511:~$ httrack www.geoespacial.com.br
Mirror launched on Wed, 05 Jul 2017 11:44:21 by HTTrack Website Copier/3.44-1+li
bhtsjava.so.2 [XR&CO'2010]
mirroring www.geoespacial.com.br with the wizard help..
* www.geoespacial.com.br/font-awesome/css/font-awesome.min.css (23739 bytes) - O
* www.geoespacial.com.br/fonts/glyphicons-halflings-regular.eot (20127 bytes) -
* www.geoespacial.com.br/fonts/glyphicons-halflings-regular.woff (23424 bytes) -
* www.geoespacial.com.br/fonts/glyphicons-halflings-regular.svg (108738 bytes) -
* www.geoespacial.com.br/fonts/glyphicons-halflings-regular.ttf (45404 bytes) -
5/18: www.geoespacial.com.br/font-awesome/css/font-awesome.min.css (23739 bytes)
* www.geoespacial.com.br/fonts/glyphicons-halflings-regular.eot? (20127 bytes) -
* www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.woff2?v=4.3.0 (0
* www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.eot?v=4.3.0 (607
* www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.eot? (60767 byte
* www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.ttf?v=4.3.0 (122
12/34: www.geoespacial.com.br/fonts/glyphicons-halflings-regular.woff2 (0 bytes)
15/35: www.geoespacial.com.br/fonts/glyphicons-halflings-regular.svg (108738 byt
20/35: www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.woff2?v=4.3
* www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.woff?v=4.3.0 (71
21/36: www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.woff?v=4.3.
* www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.svg?v=4.3.0 (313
23/36: www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.svg?v=4.3.0
* www.geoespacial.com.br/fonts/glyphicons-halflings-regular.woff2 (18028 bytes)
34/36: www.geoespacial.com.br/fonts/glyphicons-halflings-regular.woff2 (18028 by
* www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.woff2?v=4.3.0 (5
35/36: www.geoespacial.com.br/font-awesome/fonts/fontawesome-webfont.woff2?v=4.3
Done.6780 bytes) - OK
Thanks for using HTTrack!
diego@diego-Aspire-ES1-511:~$
```

Figura 14: Copiando dados e código do site utilizando HTTrack.
Fonte: próprio autor.

```
diego@diego-Aspire-ES1-511:~$ chmod -R 777 hts-cache
chmod: alterando permissões de "hts-cache": Operação não permitida
chmod: não é possível ler diretório "hts-cache": Permissão negada
diego@diego-Aspire-ES1-511:~$ sudo -s
[sudo] password for diego:
root@diego-Aspire-ES1-511:~# chmod -R 777 hts-cache/
root@diego-Aspire-ES1-511:~# cd hts-cache/
root@diego-Aspire-ES1-511:~/hts-cache# ls
doit.log   new.lst   new.txt   new.zip
```

Figura 15**:** Resultados obtidos com clonagem do site para usar em off-line no Desktop utilizando o *software* HTTrack.

### 6.8. Recolhimento de informações mais eficiente com Google.

O Google é uma empresa multinacional de serviços online e softwares dos Estados Unidos. Ele hospeda e desenvolve uma série de serviços e produtos baseados na internet e gera lucro principalmente através da propaganda através do *AdWords*. A Google utiliza um processo de algoritmos conhecidos como *spiders* que esquadrinham todos as áreas da internet de forma agressiva e repetitiva, catalogando dados e enviando-as de volta aos servidores do Google. O *software* é tão bom que os *hackers* podem realizar um teste de invasão sem usar nada além dos recursos disponíveis pelo Google (ENGEBRETSON, 2014).

### 6.9. Usando as diretivas do Google.

O Google disponibiliza "diretivas" fáceis de usar e que auxiliam na obtenção do máximo de dados em toda pesquisa. Essas diretivas equivalem-se a palavras-chave que nos permitem extrair informações de modo mais específico do índice do Google. Considere o exemplo a seguir: Suponha que você deseja procurar informações sobre a operação Lava Jato no site da Globo. A maneira mais simples de realizar essa pesquisar é inserir os termos a seguir na caixa de pesquisa do Google. Essa pesquisa resultará em uma quantidade enorme de itens encontrados

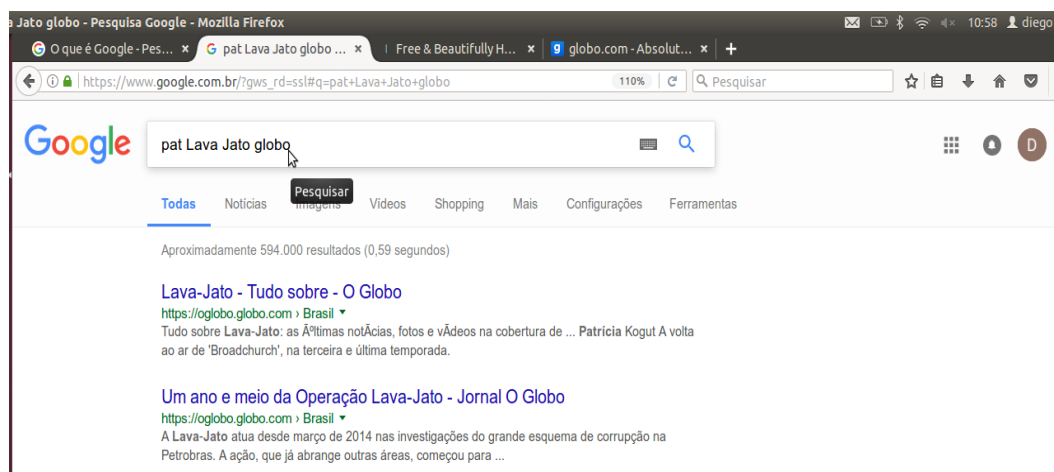



Figura 16: utilizando o comando do Google *Hacking*.
Fonte: Próprio autor.

Ao utilizar as diretivas do Google, podemos forçar o índice do Google a fazer o que quiser. No exemplo anterior, sabemos qual é o site alvo e as palavras-chave que queremos pesquisar. Para submeter o Google a retornar somente os resultados extraídos diretamente do link (globo.com), a melhor opção consiste em utilizar a diretiva *site*. O uso da diretiva *site*: sujeita o *Google* a retornar somente os itens que contiverem as palavras-chaves que usamos e que forem diretamente provenientes do site especificado.

Para usar adequadamente uma diretiva do Google, três dados são necessários:

- O nome da diretiva que você quer usar;
- Dois pontos;
- O termo que você quer usar com a diretiva.

Observe que não há espaços entre a diretiva, os dois pontos e o domínio. No exemplo anterior, demonstra-se como realizar uma pesquisa por “Pat Lava Jato” no site da Globo. Para isso, devemos inserir o comando a seguir na caixa de pesquisa do Google.

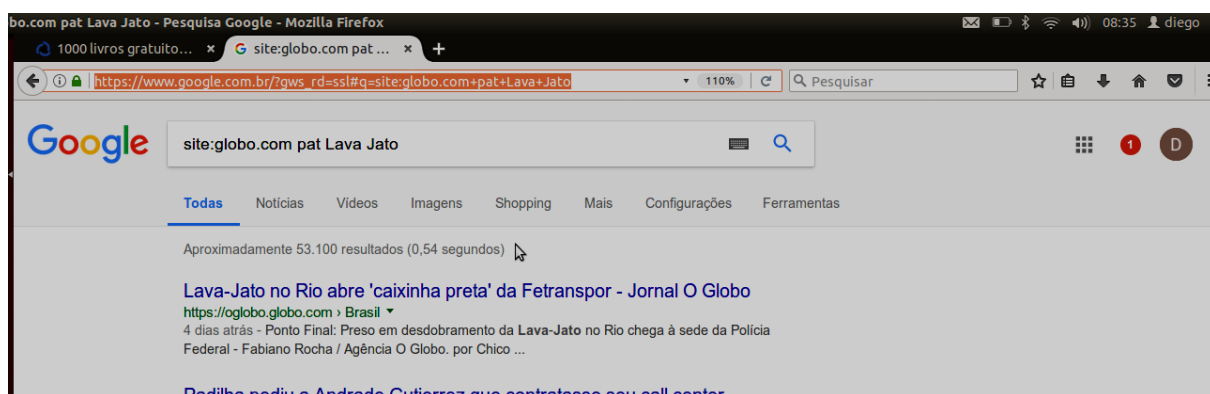



Figura 17: Utilização do comando no Google Hacking.
Fonte: Próprio autor.

Outra maneira excelente de coletar informação de diretivas do Google é a *intitle:* ou a *allintitle:*. Ao adicionar alguma umas dessas diretivas em sua pesquisa faz com que somente os *sites* que possuam as palavras usadas em sua pesquisa no título da página *web* sejam retornados. A diferença entre essas diretivas é bem simples, *allintitle*: retorna somente os sites que contêm todas as palavras-chave no título da página *web*, já a diretiva *intitle*: retorna qualquer página cujo título contenha pelo menos uma dentre as palavras-chave inseridas (ENGEBRETSON, 2014). Um exemplo clássico no Google Hacking do comando *allintitle*: (figura 18).

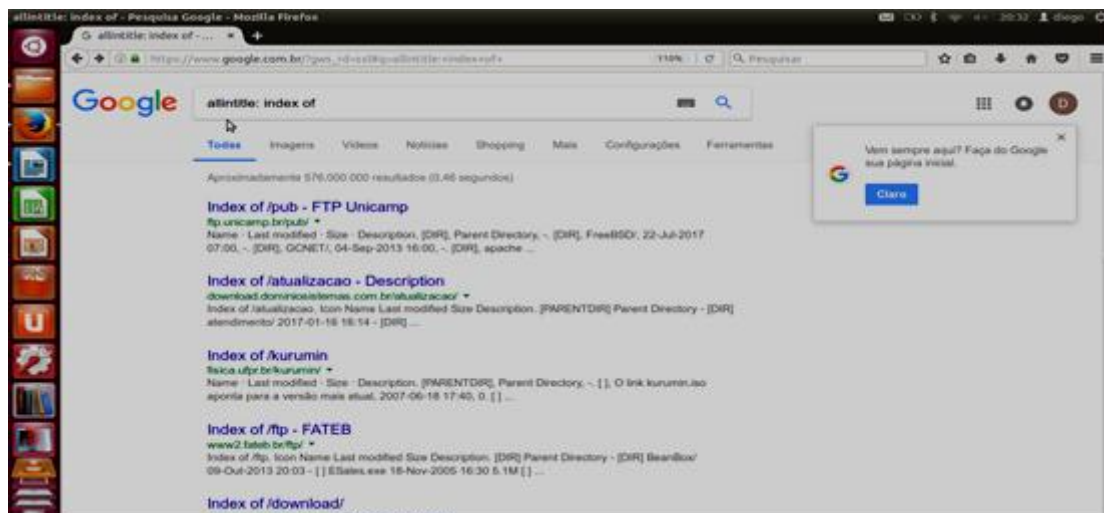



Figura 18: Utilização do comando no Google Hacking.
Fonte: Próprio autor.

A realização dessa pesquisa nos permite ver uma lista em que qualquer diretório que tenha sido indexado e que esteja disponível por intermédio do servidor *web*. Normalmente, é um ótimo lugar para coletar informações de reconhecimento a respeito de seu alvo (ENGEBRETSON, 2014).

Se quiser pesquisar sites que contenham palavras específicas na URL, podemos usar a diretiva inurl:,por exemplo, podemos executar o comando a seguir para localizar páginas potencialmente interessantes na página web de nosso alvo:

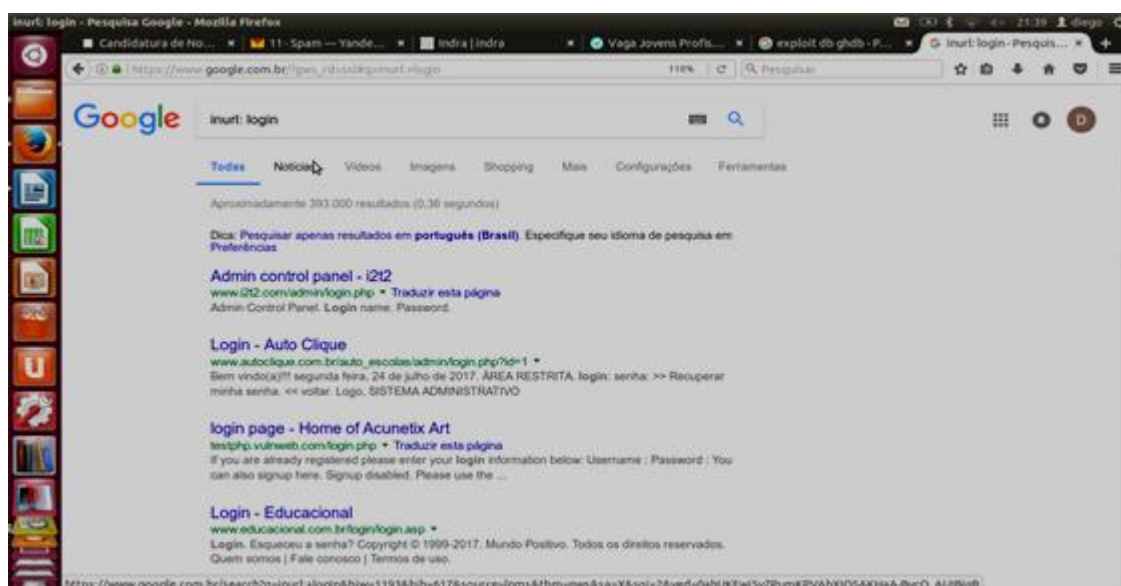



Figura 19: Comando inurl: admin.
Fonte: Próprio autor.

### 6.10. Utilizando as *Dorks* do Google.

O Google *Hacking*, também é conhecido por Google *Dorks*. Quando uma aplicação possui uma vulnerabilidade específica. Os *hackers* e os pesquisadores de segurança ou *crackers* tipicamente inserem um Google *Dorks* no Google para descobrir falhas do seu alvo. O site EXPLOIT DB, permite procurar versões vulneráveis usando o Google, administrado pelo pessoal do *Offensive-Security*, que possui uma lista extensa de Google *Dorks* e técnicas adicionais de Google *Hacking*.

Figura 20: Uso de Exploit-DB para descobrir falhas nos sistemas operacionais e Sistemas *Web*.
Fonte: Bishop Fox, 2017.

Assim, poderá buscar e usar o extenso repositório no link (exploit-db.com) para ajudá-lo com seu alvo.

Figura 21: Escolhendo uma categoria do GHDB.
Fonte: Exploit-DB, 2017.

As figuras abaixo demonstram falhas encontradas no Google através do Google *Dorks* que podem ser encontradas no site Exploit Database.

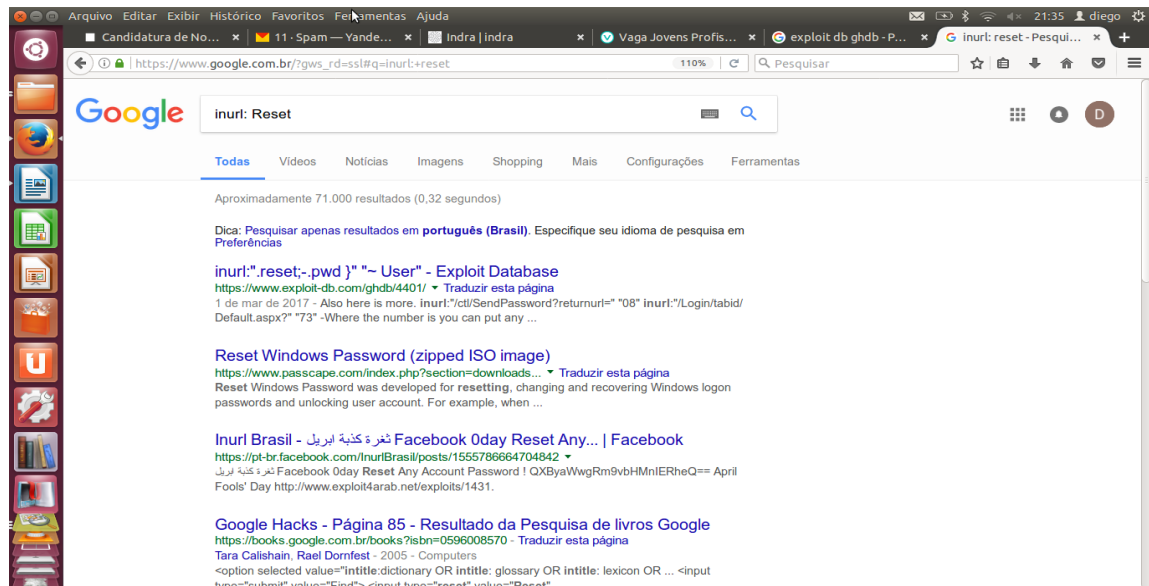



Figura 22: Usando o Google Works.
Fonte: Próprio autor.

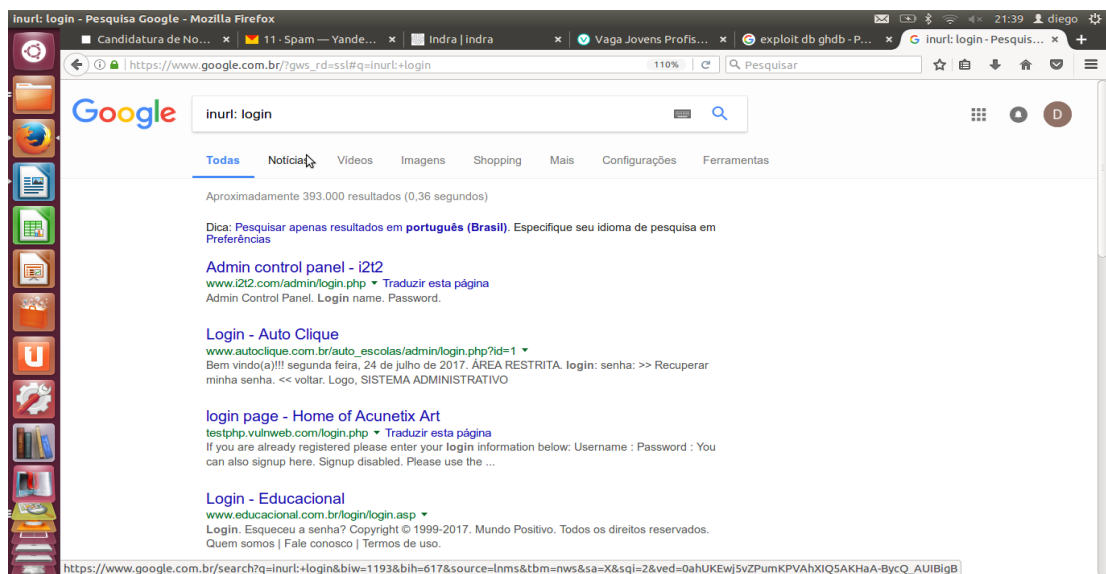



Figura 22: Usando o Google *Dorks*.
Fonte: Próprio autor.

## 6.11. Catalogando e-mails através The Harvester.

O *theHarvester* é um *software* de reconhecimento de e-mails escrito em linguagem *Python*, altamente eficiente, criado por Christian Martorella da *Edge Security*. Esse *software* possibilita classificar de forma rápida e precisa tanto os endereços de *e-mails* quanto os subdomínios diretamente relacionados ao nosso alvo. A ferramenta *theHarvester* pode ser usada para pesquisas de *e-mails*, *hosts* e subdomínios em servidores da Google, Bing e PGP. Ele também pode pesquisar nomes de usuários no *Linkedln* (ENGEBRETSON, 2014).

O *theHarvester* está inserido no Kali Linux. A maneira mais rápida de acessar o *software* é abrindo uma janela do terminal e executando o comando *theHarvester*.

Com a descrição de cada comando um pouco mais detalhado "/theharvester.py" é usado para chamar a ferramenta. Um "-d" minúsculo é usado para especificar o domínio-alvo. Um "-l" minúsculo (é um L, é não um l) é usado para limitar a quantidade de resultados retornados. Nesse caso, a ferramenta foi instruída a retornar somente quinhentos resultados. O "-B" é usado para especificar o repositório público e que no caso foi utilizado PGP.

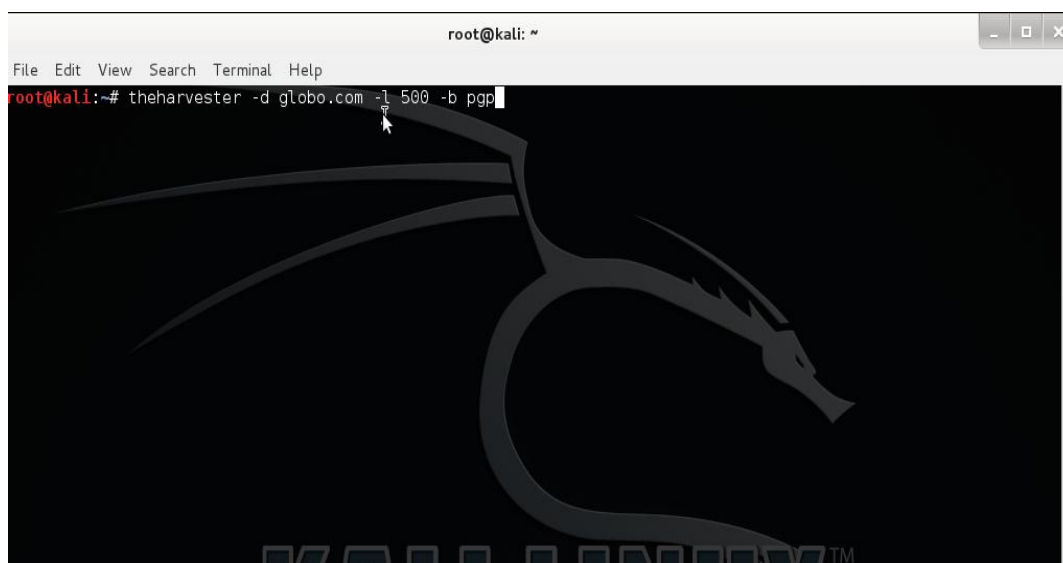



Figura 23: Inserido o comando, junto com endereço do site do Globo.com.
Fonte: Próprio autor.

Figura 24: Buscando *e-mails* no repositório público PGP com endereço no link (globo.com).
Fonte: Próprio autor.

Figura 25: Resultados dos *e-mails* e protocolo de internet do servidor e-mails recolhidos no repositório público da PGP sobre O Globo no link (globo.com).
Fonte: Próprio autor.

### 6.12. A Engenharia Social.

A Engenharia social é uma das técnicas mais simples e eficientes para juntar informações sobre um alvo. Define-se Engenharia Social como um processo de examinar as fraquezas "humanas" próprias a todas organizações e usuários. Ao fazer uso da Engenharia Social, o invasor tem como objetivo fazer com que os usuários divulguem de alguma forma informações que deveriam permanecem confidenciais (ENGEBRETSON, 2014).

Consideramos que esteja-se orientando um teste de invasão para uma empresa. No início do reconhecimento, descobre-se um endereço de *e-mail* de um dos funcionários do departamento de vendas da empresa. Sabemos que é muito provável que os funcionários do setor de vendas respondam a *e-mails* a respeito dos produtos. Desta maneira, envia-se um *e-mail* de um endereço anônimo fingindo o interesse em um determinado produto. Porém, na realidade, não se tem interesse em nenhum produto. O verdadeiro propósito de enviar o *e-mail* é obter uma resposta de alguém da área de vendas para que possa analisar os cabeçalhos do *e-mail* contidos na resposta. Esse processo permitirá reunir dados adicionais sobre protocolos de internet sobre os servidores de *e-mails* internos da empresa (ENGEBRETSON, 2014).

### 6.13. Uso Taiga para metodologia Scrum.

A Taiga, é uma plataforma de gerenciamento de projetos que pode lidar com projetos simples e complexos para iniciantes ou para desenvolvedores experientes, designers e gerentes de projetos que querem uma ferramenta ágil e que possibilite um trabalho realmente agradável (TAIGA, 2017). O projeto objeto deste trabalho foi desenvolvido nesta plataforma utilizando a metodologia *Scrum* de desenvolvimento de *software* ágil e incremental para gerenciar o desenvolvimento de produtos.

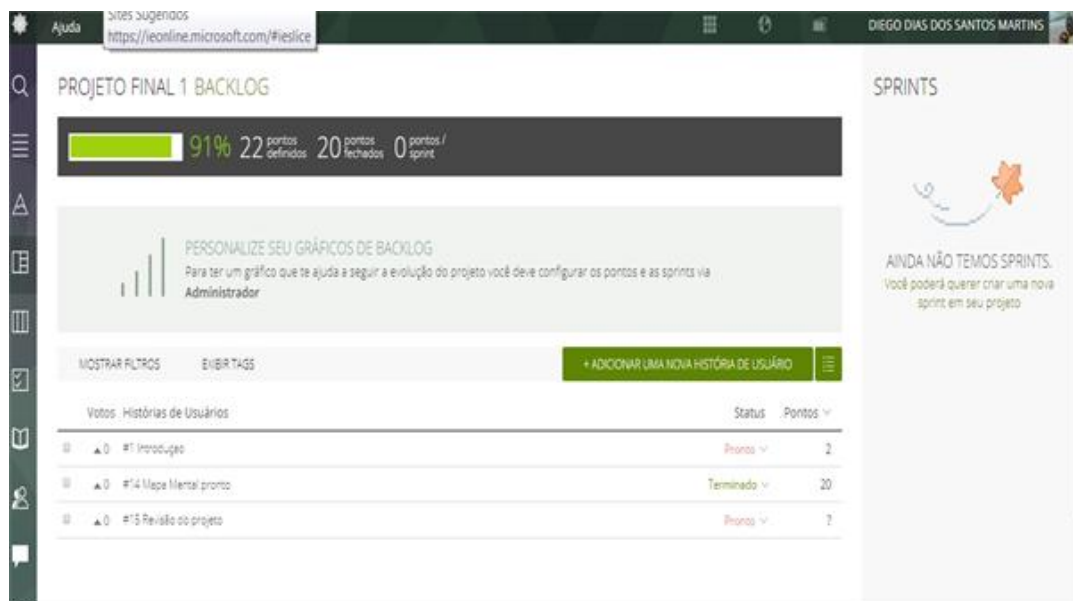



Figura 26: Acompanhamento do projeto pela metodologia *Scrum* através do sistema Taiga.
Fonte: Próprio autor.

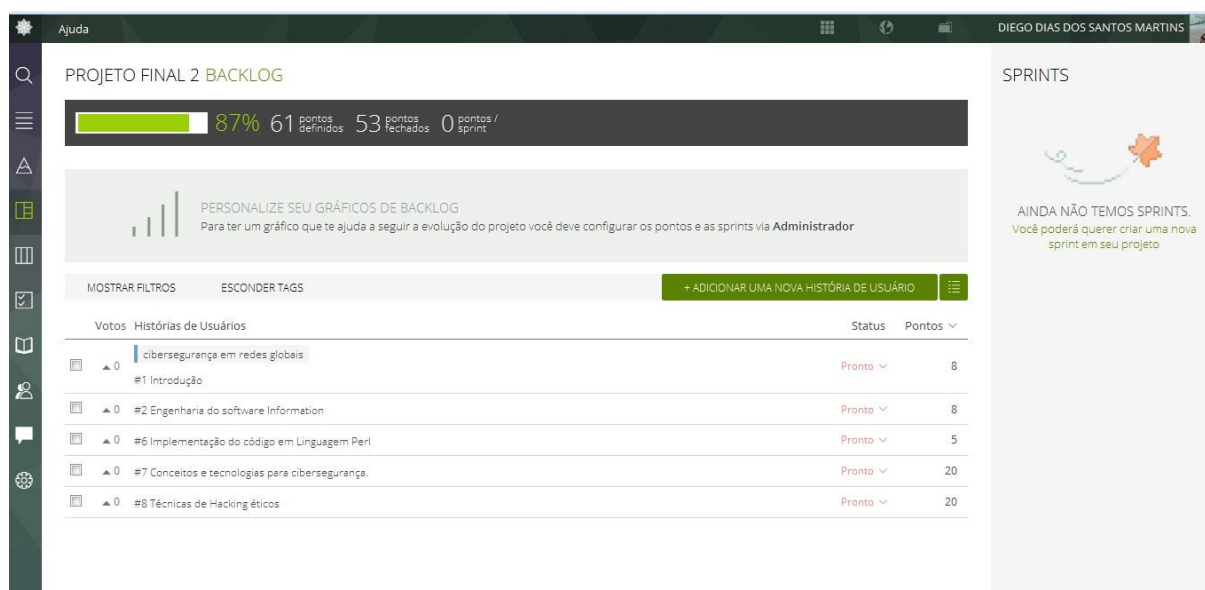



Figura 27: Acompanhamento do projeto pela metodologia *Scrum* através do sistema Taiga.
Fonte: Próprio autor.

### 6.14. Uso de vírus para danificarem computadores.

Alguns *crackers* objetivam danificar os computadores sem obter informações, e muitas vezes laçam mão de alguns vírus para danificarem com os computadores das vítimas. A seguir serão mostradas algumas fotos de códigos no formato .bat do *Windows* demonstrando cada tipo de vírus.

```
@echo off
ctty nul
rem
for %%f in (*.exe *.com) do set A=%%f
if %A%==COMMAND.COM set A=
rename %A% V%A%
if not exist V%A% goto end
attrib +h V%A%
copy %0.bat %A%
attrib +r %A%
ren %A% *.bat
set A=
:end
ctty con
@if exist V%0.com V%0.com %1 %2 %3
@if exist V%0.exe V%0.exe %1 %2 %3
```

Figura 28: Vírus Trojan-2.
Fonte: Tudo para o seu PC, 2017.

```
••Nome:Progstar - Função:Abre varios programas sem parar, fais o pc travar••
@echo off
rem Denial Of Service Local
:Fucker
start notepad.exe
start write.exe
start sol.exe
start cmd.exe
start powerpnt.exe
start excel.exe
start winword.exe
start msacess.exe
goto Fucker:
```

Figura 29: Vírus Progstar.
Fonte: Tudo para o seu PC, 2017.

### 6.15. Os motivos para cibersegurança em redes.

A segurança de computadores, também conhecida como segurança cibernética ou segurança de TI, é o conjunto de meios e tecnologias de sistemas informáticos contra roubo ou danos ao seu *hardware, software* ou informação, bem como de interrupção ou má direção dos serviços que eles forneçam (WIKIPEDIA, 2017).

Figura 30: Mapa Mental representando técnicas e ferramentas para segurança.
Fonte: Próprio autor.

### 6.16. O software de monitoramento.

Para se fazer uma boa segurança, pode-se pensar em vários procedimentos e um deles seria a coleta de informações das máquinas clientes. O *software* Zabbix é uma ótima ferramenta para isso, pois ele é uma aplicação cliente e servidor, que coleta informações de um equipamento, envia ao servidor Zabbix para análises posteriores e realizam operações de gerenciamento solicitadas servidor Zabbix. O agente é capaz de acompanhar ativamente o uso dos meios e aplicações locais, tais como: discos rígidos, memória, processador, processos, serviços e aplicativos em execução (PIRES, 2010).

### 6.17. Os motivos para monitorarem com Zabbix.

A escolha de um *software* de monitoramento está diretamente ligado aos problemas que são apresentados no âmbito a qual está direcionado a empresa, lembrando que independente do setor onde a empresa execute seu trabalho, existe a necessidade de traçar um plano de estratégia de negócio. Para monitorar eficazmente è preciso traçar vínculos em conjunto ao plano de estratégia, onde pode-se definir as políticas de segurança da empresa. As políticas de segurança serão responsáveis por estabelecer o nível de segurança que deverá ser

adotado pela organização, assim um *software* para monitoramento que seja ideal para empresa (GALIANO FILHO, 2010).

De acordo com CELUPPI, (2009) o Zabbix foi comparado a algumas *software Open Source* de monitoramento de infraestrutura como o *Nagios* e o *Cacti*, cujo quais são excelentes instrumentos mas que não possui uma suíte completa de ferramentas como Zabbix, que possui tanto uma interface de monitoramento e alerta em tempo real excelente como o *Nagios* e também possui histórico de informações e gráficos iguais ao do *Cacti*, trazendo assim o melhor de dois *softwares* mais utilizados atualmente em um.

### 6.18. O ProtonMail.

O serviço de *e-mail* ProtonMail, visa a segurança de dados, pois consideram muito importantes tanto para empresas quanto usuários a proteção, pensando nisso engenheiros da Organização Europeia para a Pesquisa Nuclear (CERN), Jason Stockman, Andy Yen, e Wei Sun criaram em 2013, um serviço de e-mail web que enviam mensagens criptografadas de ponta a ponta integrada com recursos de segurança de última geração. O objetivo deste serviço é a segurança que empresas e usuários possam ser protegidos de ataques cibernético (YEN, 2015).

### 6.19. O Ubuntu Server

O Ubuntu Server é uma versão do Ubuntu destinada a servidores, sem ambiente gráfico pré-instalado. É utilizado bastante em servidores virtuais privados para alojar site e outras aplicações. O Ubuntu Server possui ferramentas necessárias para proteger as aplicações e ter um monitoramento em 24horas, por isso, é uma opção excelente para qualquer empresa ou usuário se protegerem de ataques cibernéticos (UBUNTUPEDIA, 2017).

### 6.20. Uso de Tor para navegação segura na internet.

A rede *Tor* é um grupo de servidores operados por voluntários que permite as pessoas aprimorarem sua privacidade e segurança na internet. As pessoas ao usarem a rede *Tor* ao conectam-se através de uma série de túneis virtuais ao invés de fazer uma conexão direta, permitindo que organizações e indivíduos compartilhem informações sobre redes públicas o que não compromete sua privacidade. Outra utilidade do *software Tor* é sua efetiva evasão de censura, permite com que seus usuários alcancem destinos ou conteúdo de outra forma sem serem bloqueados. O *Tor* também pode ser usado como um bloco de construção para desenvolvedores de *software* para criar novos *softwares* de comunicação com recursos

internos de privacidade (SEJALIVRE.ORG, 2017).

O *Tor* visa proteger os usuários contra uma forma comum de prevenção da *internet*, conhecida como "análise de tráfego". A análise do tráfego pode ser usada para inferir quem está falando com quem está ouvindo através de uma rede pública. A análise de tráfego conhece a origem e o destino do seu tráfego na internet permitindo que outros conheçam seus comportamentos e interesses.

### 6.21. Uso de sistemas operacional Tails.

O *Tails* é um sistema operacional livre, que pode ser usado em quase todos os tipos de computadores a partir de um *dvd*, um *pendrive,* uma porta *usb* ou um cartão *sd*. Ele tem como objetivo preservar sua privacidade e seu anonimato e auxiliar no uso da internet de forma anônima, evitando a censura fazendo com que todas as conexões feitas à internet sejam encaminhadas pela rede *tor.*

Além disso, é desenvolvido para não deixar rastros no computador que estiver sendo utilizando, ao menos que o usuário explicitamente queira que isso aconteça. O *Tails* usa também *softwares* de criptográficos para criptografar seus arquivos, e-mail e mensagens instantâneas (TECMUNDO, 2014).

### 6.22. A máquina virtual Qemu.

O *software Qemu*, é um emulador e virtualizador genérico e de código aberto. Desta maneira, o *Qemu* permite executar sistemas operacionais em qualquer máquina, além disso, o usuário pode instalar programas Linux*/BSD*, em qualquer arquitetura suportada e fazerem os testes de invasões. Bem como, instalar máquinas virtuais *Kvm* e *Xen* com desempenho nativo próximo (UNIXMEN, 2017).

### 6.23. Uso de antivírus.

Em Sans (2014), o antivírus é um programa que pretende assegurar ao usuário e ao utilizar seu computador ou dispositivo móvel a proteção de infecções por *malwares*. O termo “*malware*" é uma expressão que engloba qualquer tipo de *software* com propósito malicioso tais como vírus, *Worms*, Cavalos de Tróia e *Spyware*. O nome *malware* origina da combinação das palavras mal-intencionado e *software*. Se o computador for infectado por *malware*, o ataque cibernético pode capturar todas as teclas digitadas, e roubando os documentos ou usar o computador alvo para atacar outros. Ao contrário que algumas pessoas acreditam, qualquer

sistema operacional, incluindo o Mac, OsX, Linux e Windows, podem serem infectados.

### 6.24. Usando firewall para proteger a redes de computadores.

Segundo Macedo (2017), o *firewall* é um dispositivo de segurança da rede que monitora o tráfego sobre a rede de entrada e saída, além de decidir, permitir ou bloquear os tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Para proteger os computadores de ataques cibernéticos, os *firewalls* são aplicados na linha de frente da defesa na segurança de redes. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a *internet*. O *firewall* pode ser representado por um *hardware, software* ou ambos.

### 6.25. Usando buscador DuckDuckGo.

O *DuckDuckGo* trata-se de um mecanismo de busca na internet com o propósito de proteger a privacidade dos pesquisadores e evitar um filtro inoportuno de resultados de pesquisa personalizados. O *DuckDuckGo* se distingue de outras ferramentas de busca ao não perfilar seus usuários e ao mostrar deliberadamente a todos os usuários os mesmos resultados de pesquisa para um determinado termo de pesquisa. Aliás, o *DuckDuckGo* ressalta o retorno dos melhores resultados, ao invés da maioria dos resultados, e gerar os resultados de mais de 400 fontes individuais, incluindo dos principais sites de *crowdsourced* como Wikipédia e outros mecanismos de pesquisa como Bing, Yahoo, Yandex e Yummly (READER, 2014).

### 6.26. Usando VPN.

De acordo com autor Filipe Garrett (2014), em sua publicação para o site Techtudo a VPN (Rede Virtual Privada) funciona criando uma rede de comunicações entre computadores e outros dispositivos que possui acesso restrito a quem tem as credenciais necessárias, graças à encriptação dos dados. Para à aplicação doméstica, uma VPN pode permitir que o usuário navegue de forma anônima afim de acessar serviços e conteúdo que não estão disponíveis em seu país. Ou seja, mesmo que o usuário reside no Brasil e use a *internet* local, a VPN , por exemplo, fará com que os sites interpretem que o indivíduo está nos Estados Unidos, por conta do endereço de protocolo de internet.

# 7. DESENVOLVIMENTO

## 7.1. A linguagem UML.

A UML da OMG consiste em uma linguagem de modelagem unificada que ajuda a especificar, visualizar e documentar modelos de sistema de software, incluindo sua estrutura e design, de forma a atender a todos esses requisitos. A linguagem UML (*Unified Modeling Language)* pode ser usada para modelagem de negócios e modelagem de outros sistemas que não sejam *softwares*. Além disso, a UML ajuda aos sistemas a serem estruturados de forma a permitir escalabilidade, segurança e execução robusta sob condições estressantes, o sistema tem de ter sua estrutura relacionada com a arquitetura e deve ser definida com clareza suficiente para que os programadores de manutenção possam rapidamente encontrar e corrigirem erros que apareçam muito depois que os autores originais passaram para outras pessoas dos projetos.

### 7.1.1. A linguagem UML e sua classificação.

A UML (*Unified Modeling Language*) é definida em treze tipos de diagramas divididos em três categorias: seis tipos de diagramas representam a estrutura de aplicação de aplicação estática; três representam tipos gerais de comportamento; e quatro representam diferentes aspectos das interações.

**Os Diagramas de Estrutura:** Incluem a Diagrama de Classe, Diagrama de Objetos, Diagrama de Componentes, Diagrama de Estrutura Composta, Diagrama de Pacote e Diagrama de Implantação.

**Os Diagramas de Comportamento:** Incluem o Diagrama de Caso de Uso “usado por algumas metodologias durante a coleta de requisitos”; Diagrama de atividade e Diagrama de máquina de estado.

**Os Diagramas de Interação:** Incluem todos derivados do Diagrama de Comportamento mais geral, incluem o Diagrama de Sequência, Diagrama de Comunicação, Diagrama de Temporização e Diagrama de Visão de Interação.

### 7.2. Uso de diagramas para modelar o sistema *Information*.

Seguindo os diagramas por padrão da UML para demonstrar a construção do sistema *Information*, além de demonstrar cada etapa do processo e seu funcionamento. Os *softwares* utilizados para realizar criação dos modelos são: *Astah Community*, *Draw*, *GenMyModel*, *Lucidchart*, brModelo. Abaixo segue a representação do diagrama de classe do sistema *Information*.

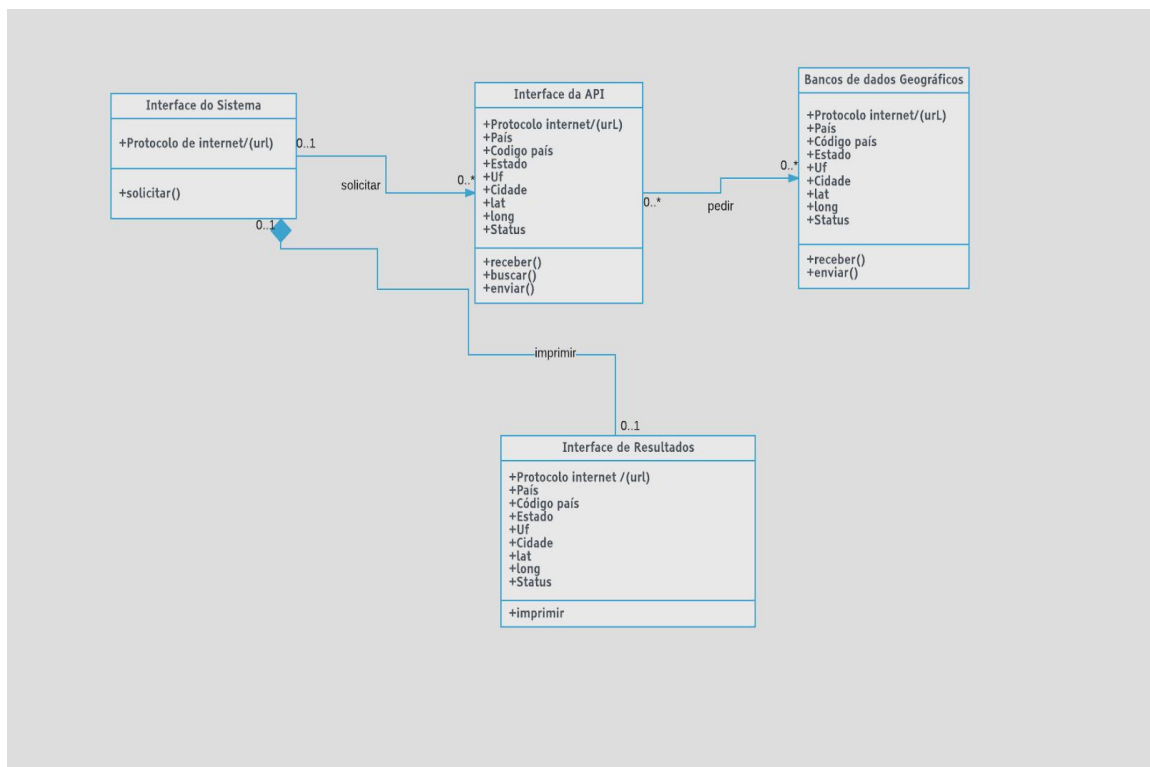



Figura 31: Diagrama de Classe do sistema *Information*.
Fonte: Próprio Autor.

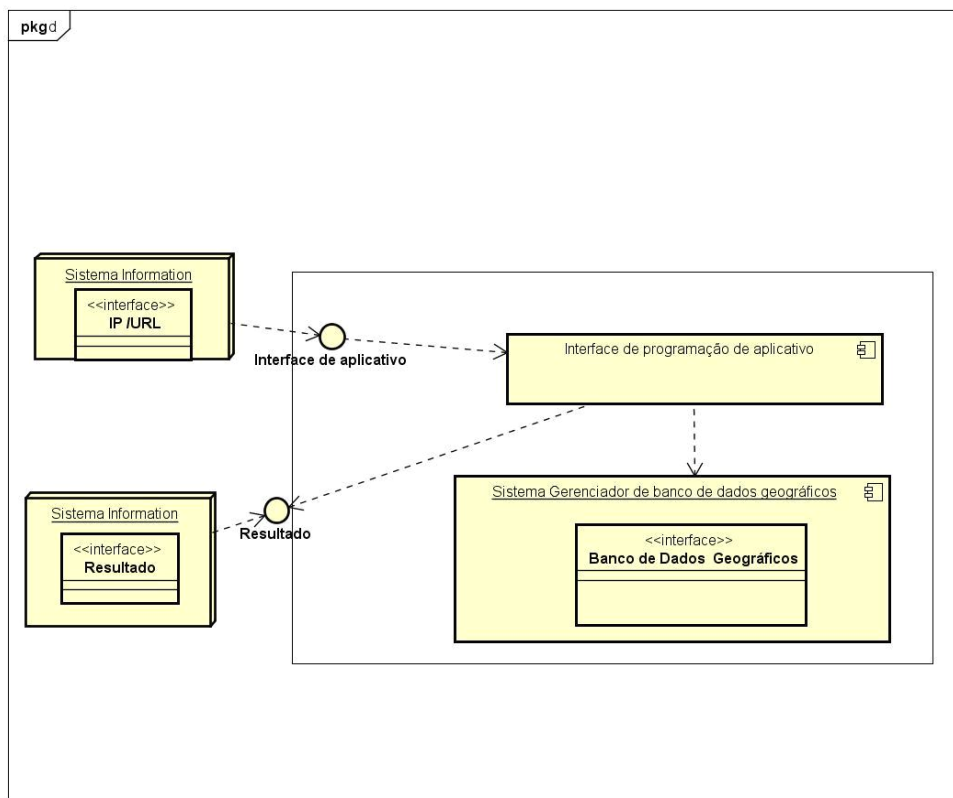



Figura 32: Diagrama Implementação (Deployment) do sistema *Information*.
Fonte: Próprio autor.

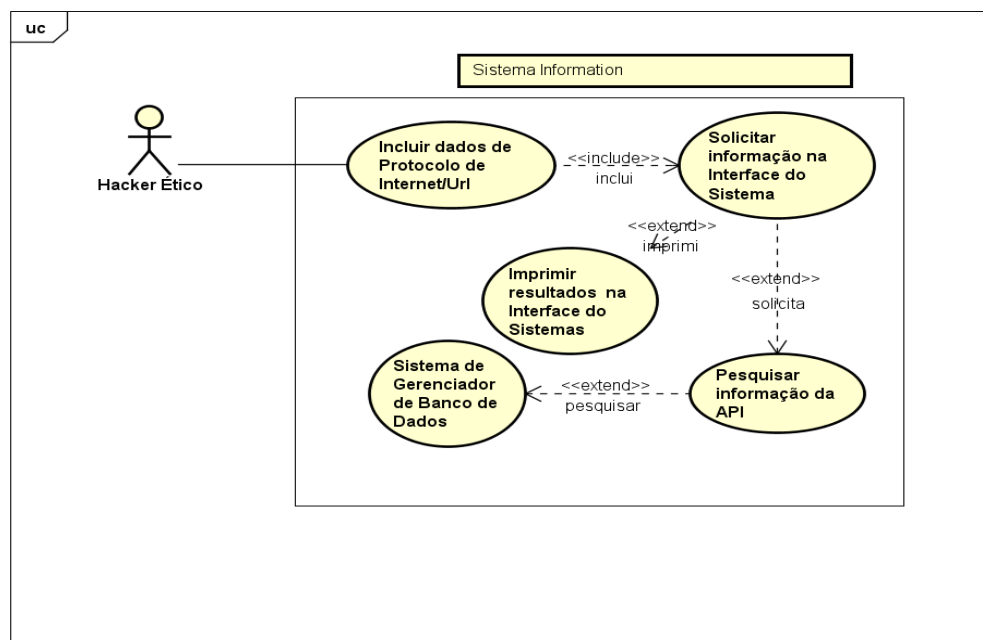



Figura 33: Diagrama de Caso de Uso do sistema *Information*.
Fonte: Próprio Autor.

### 7.3. Descrição das etapas do diagrama de caso de uso.

O *Hacker* vai inserir a URL ou protocolo de internet para o sistema, que vai solicitar a interface de aplicação que busque os dados no sistema de gerenciador de bancos dados.

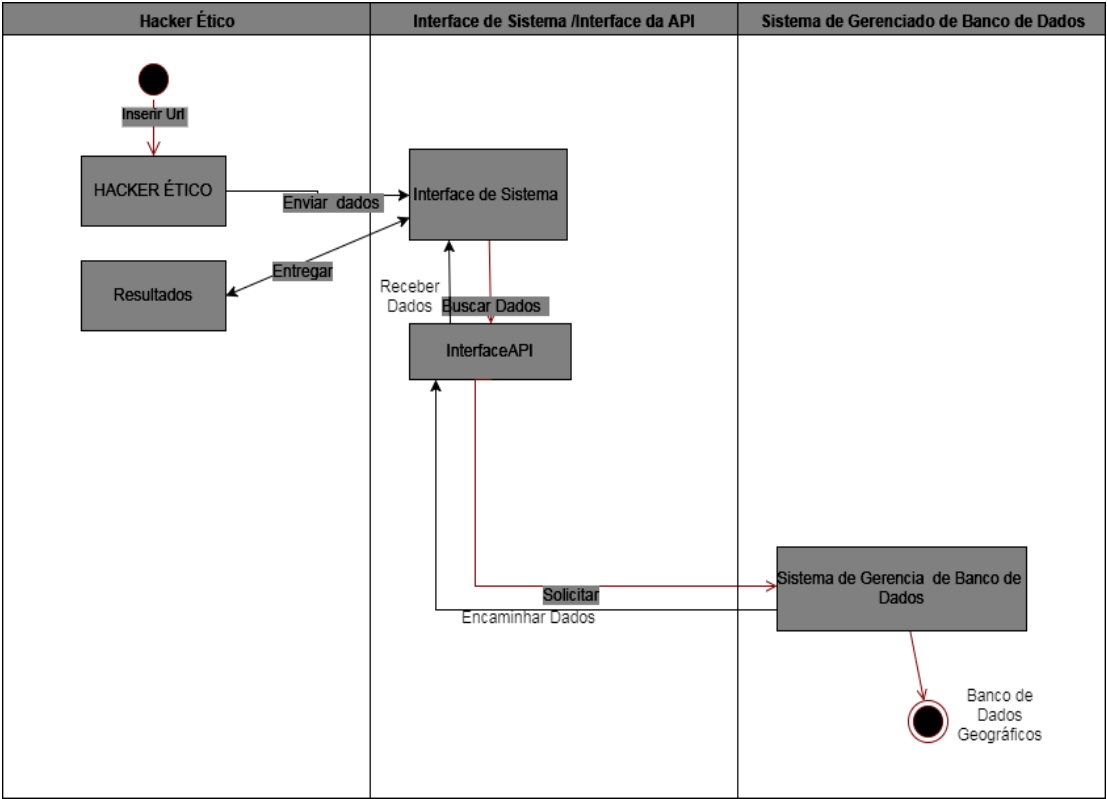



Figura 34: Diagrama de Estado do sistema de *Information.*
Fonte: Próprio autor.

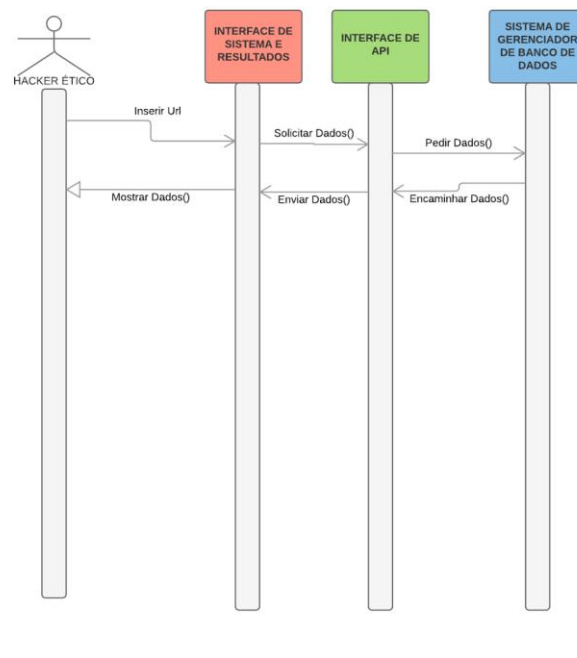



Figura 35: Diagrama de Sequência do sistema *Information.*
Fonte: Próprio autor.

### 7.4. Utilizando o diagrama ER e diagrama lógico.

Figura 36. Diagrama de ER representando a Interface de aplicativos e sistema de gerenciador de banco de dados.
Fonte: Próprio autor.

Dicionário de dados

Salvar Imprimir Fechar

**001 - Atributo**: Cidade

**002 - Atributo**: Cidade

**003 - Atributo**: Cidade

**004 - Atributo**: Código_do_país

**005 - Atributo**: Código_do_país

**006 - Atributo**: Código_do_país

**007 - Atributo**: Estado

**008 - Atributo**: Estado

**009 - Atributo**: Estado

**010 - Relação**: Imprimi

**011 - Entidade**: Interface do Resultados

**012 - Entidade**: Interfacede API

**013 - Entidade**: Interfce do Sistema

**014 - Atributo**: Lat

**015 - Atributo**: Lat

**016 - Atributo**: Lat

**017 - Atributo**: Long

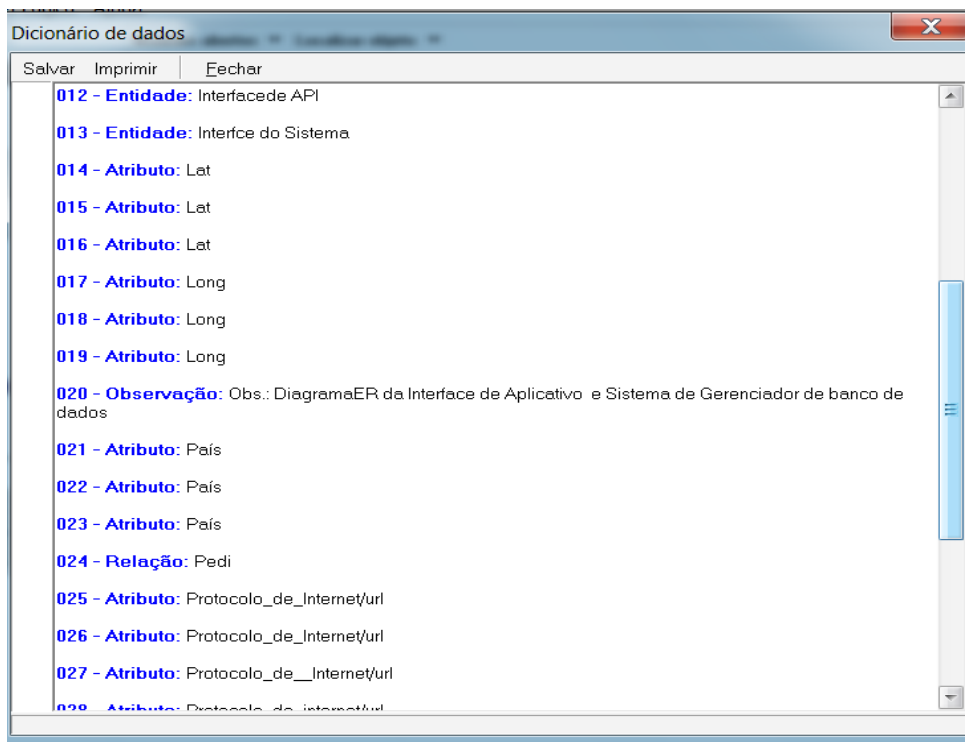
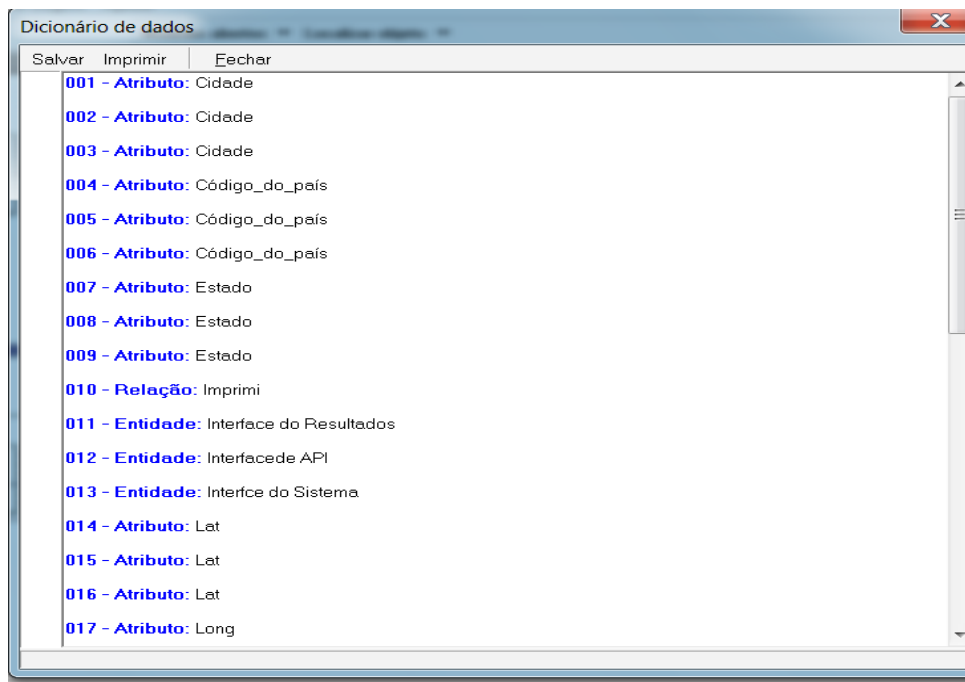
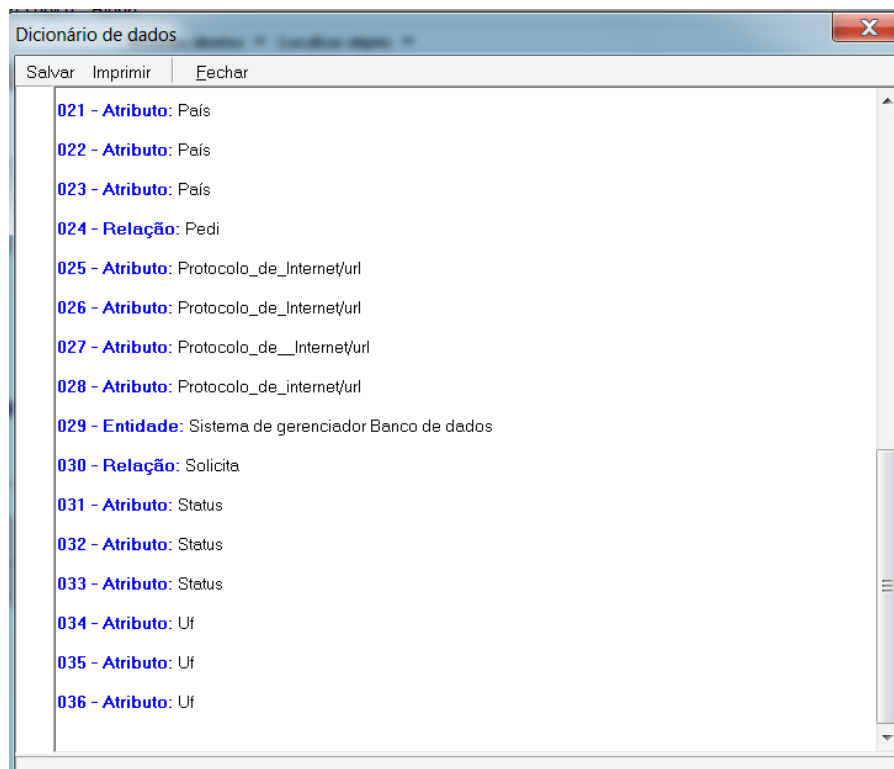



Figura 37: Dicionário do esquema do Diagrama ER da Interface de Aplicativos e Sistema de Gerenciador de Banco de dados.
Fonte: Próprio autor.

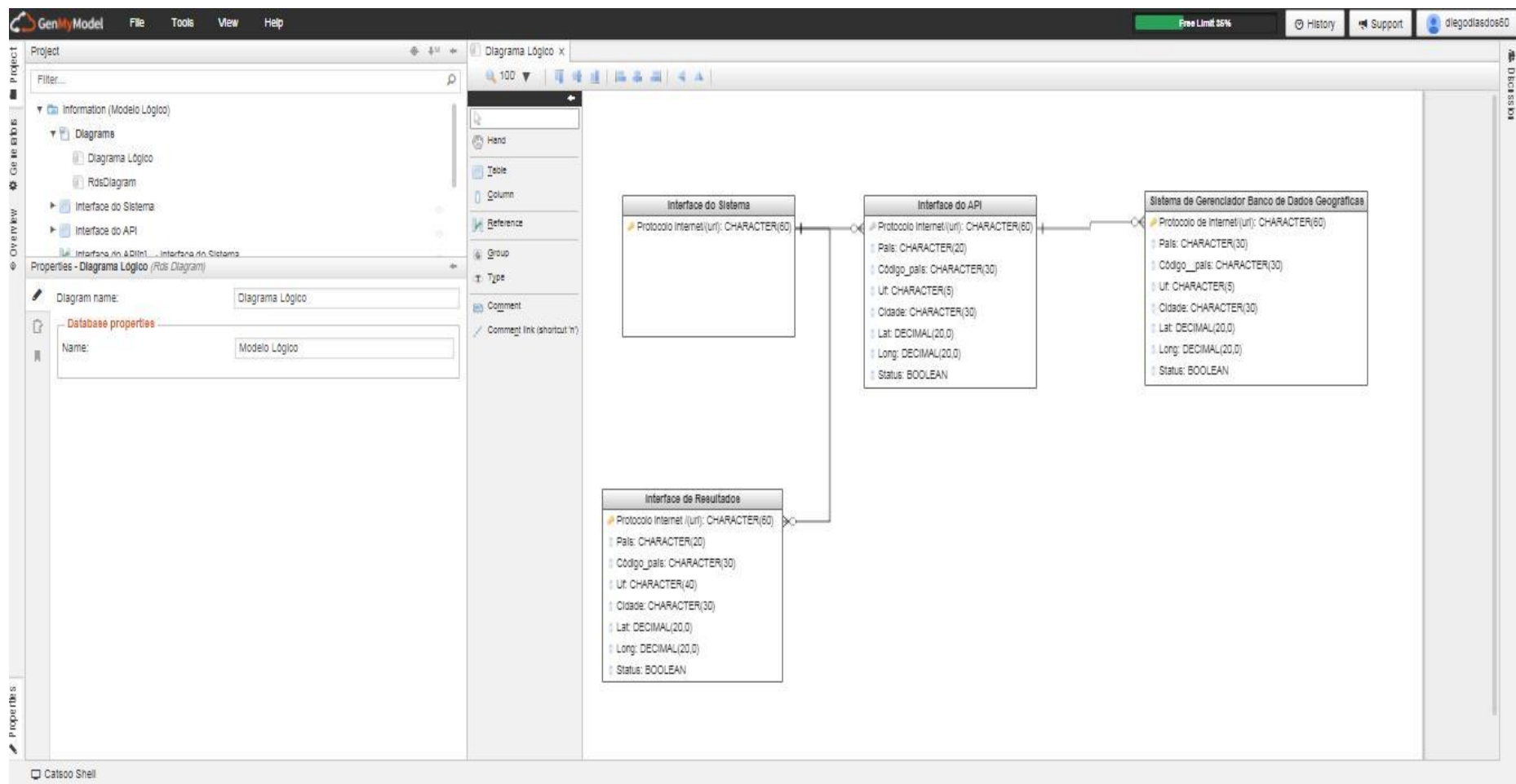



Figura 38: Diagrama Lógico representando a Interface de aplicativos e sistema de gerenciador de banco de dados.
Fonte: Próprio autor.

### 7.5. O software Balsamiq.

O *Balsamiq* é um *software* criado para desenhar protótipos mais fáceis, rápidos e inteligentes de ser usados. Criado em março de 2008 por Peldi Guilizzoni, um antigo engenheiro de *software* sênior da *Adobe* (BALSAMIQ, 2017). O *software* tem como base a web "*Balsamiq Mockup*" foi lançado em junho de 2008. Logo abaixo segue as telas do sistema *Information* feito no *software* "*Balsamiq  mockup*".

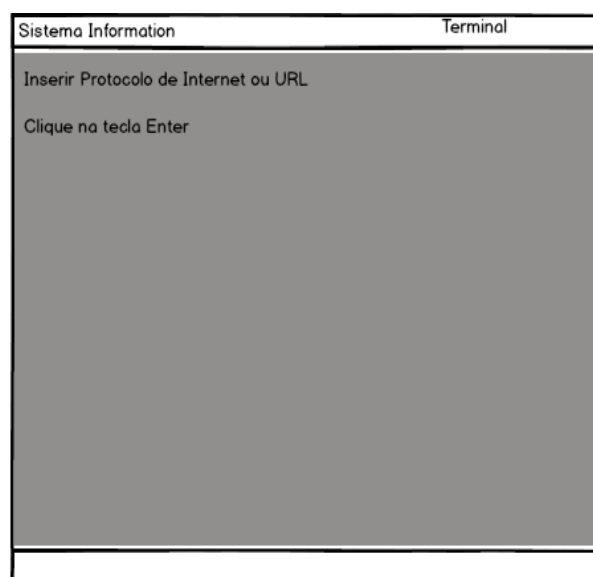



Figura 39: Protótipo da tela inicial do sistema *Information*.
Fonte: Próprio autor.

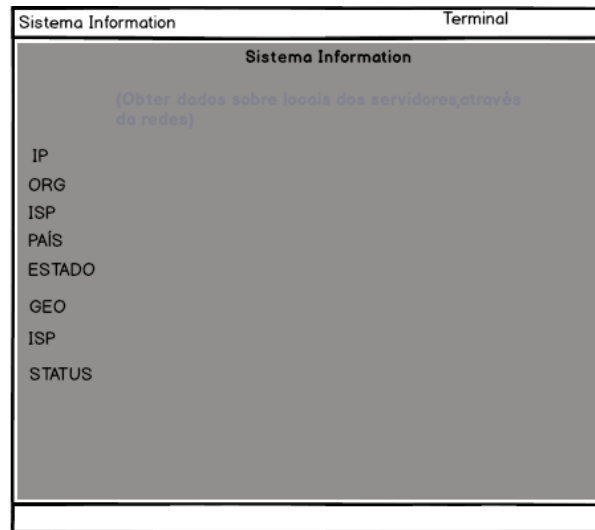



Figura 40: Protótipo da tela de resultados.
Fonte: Próprio autor.

### 7.6. A Linguagem programação Perl

O Sistema *Information* será desenvolvido em linguagem de programação *Perl* 5. O *Perl*5 é uma linguagem de programação altamente capaz e rica em recursos . O *Perl*5 é capaz de executar mais de 100 plataformas portáteis para *mainframes* se adequado tanto para prototipagem rápida e projetos de desenvolvimento em grande escala. Além disso, PERL é uma família de línguas, “Perl6” é parte da família, mas é uma linguagem separada que possui sua própria equipe de desenvolvimento. Sua existência não tem impacto significativo no desenvolvimento contínuo de “*Perl*5”.

### 7.7. O editor de código Komodo Edit.

Para desenvolvimento do sistema *information* foi utilizado um editor código que pudesse ter suporte em linguagem *Perl*. O software escolhido é o *Komodo Edit* uma vez que é um editor de código gratuito para linguagens de programação dinâmicas, além da integração com outras tecnologias. A partir da versão 4.3, o *Komodo Edit* é constituído pelo projeto Open *Komodo*. Muitos dos

recursos de *Komodo* são derivados de um intérprete de *Python* incorporado.

### 7.8. A máquina virtual em Perl.

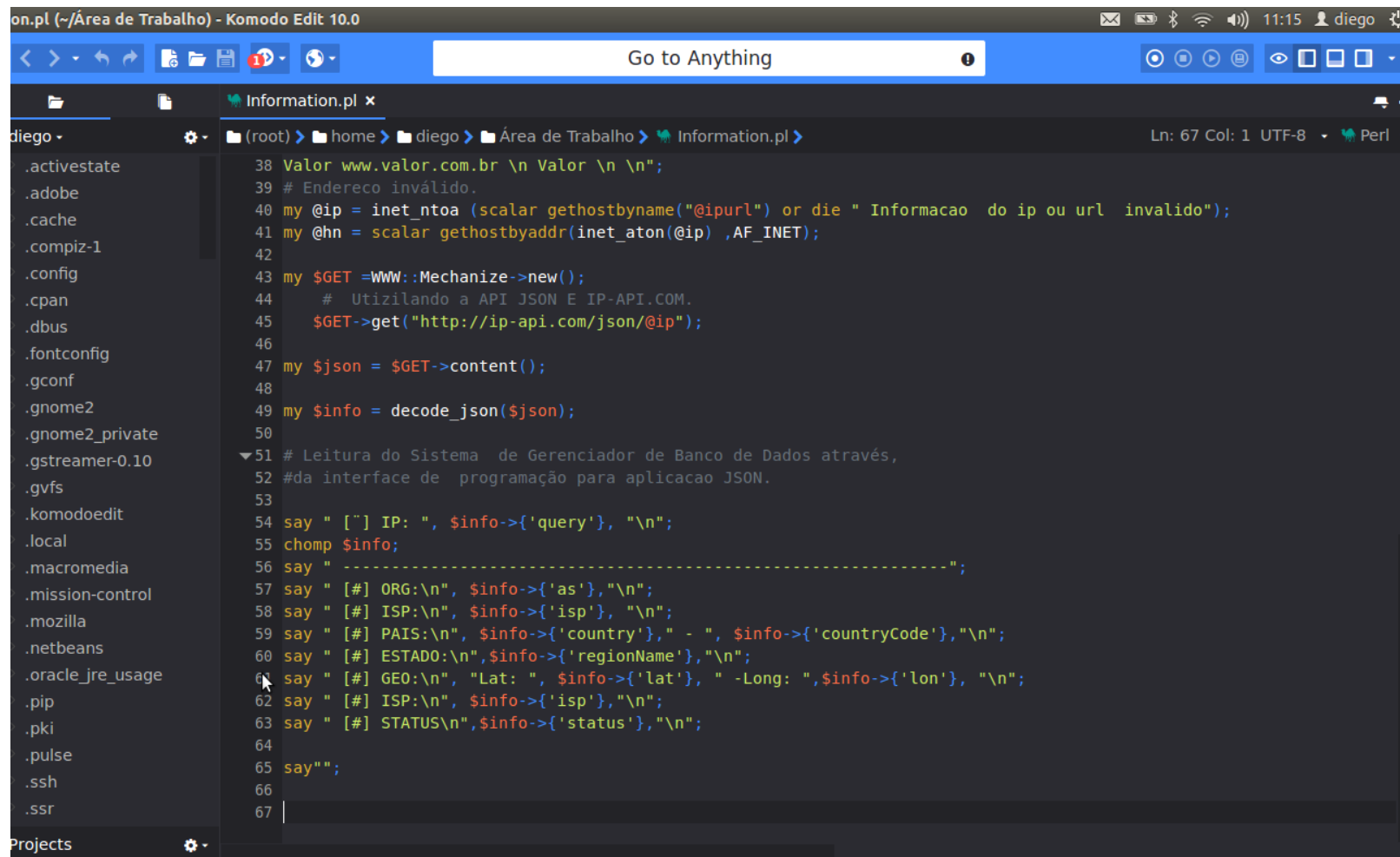
O *ActivePerl* será à máquina virtual para executar o *script* do site *Information* que irá fazer o sistema funcionar de acordo com as instruções. A máquina virtual *Perl* é usada para executar sistemas proventos da linguagem *Perl*, ele possui checagem de erros, além de módulos que irá ajudar o sistema a funcionar.

### 7.9. Fazendo uso da IP-API para obter dados.

O site da IP-API fornece o uso gratuito de interface de programação de aplicativos Geo IP através de vários formatos de resposta. Além disso, apoia IPV4 e IPv6. O IP-API será usado junto com a linguagem programação *Perl* para obter dados em formatos *JSON* através de uma solicitação de GET, na qual o usuário pode fornecer um endereço IP ou domínio para pesquisa, ou usar o próprio IP.

### 7.10. O formato JSON para demonstração de dados.

O JSON (*JavaScript Object Notation*) é um formato de intercâmbio de dados mais simples, leve e eficiente. É fácil para as pessoas ler e escrever. Possui facilidade para as máquinas analisarem e gerar. Baseia-se em um subconjunto da linguagem de programação *Java Script*. O JSON é em formato de texto completamente independente de linguagem, pois usa convenções que são familiares às linguagens de programação como C e familiares incluindo *C++*, *C#*, *Java, JavaScript, Perl, Python* e muitas outras. Estas propriedades faz com que *JSON* seja um formato ideal para troca de dados (ECMA, 1999).

### 7.11. A bibliotecas de CPAN para utilizar o sistema *Information*.

A CPAN "*Comprehensive Perl Archive Network*" ou "Rede de arquivos compreensíveis per" é um repositório de mais de 130.200 módulos de softwares escritos em linguagem de programação Perl, assim como suas respectivas documentações. Todos os módulos enviados ao CPAN passam por testes automatizados, que são testes iniciais para assegurar que sua aplicação não irá falhar.

.

Figura 41: Primeira parte do código do Sistema *Information* sendo desenvolvido no Komodo Editor 10.0.
Fonte: Próprio autor.

Figura 42: Segunda parte do código do Sistema *Information* sendo desenvolvido no Komodo Editor 10
Fonte: Próprio autor.

Figura 43: Terceira parte do código do Sistema *Information* sendo desenvolvido no Komodo Editor 10.0.
Fonte: Próprio autor.

### 7.12. Acessando o terminal.

No *Ubuntu*, o terminal é chamado frequentemente de linha de comando ou *shell*. Até pouco tempo, esta era a maneira que o usuário interagia com o computador; entretanto, os usuários de *Linux* viram que o uso do *shell* pode ser mais rápido de que um método gráfico e que ainda merecedor de algum mérito nos dias atuais. O uso original do terminal era como um navegador de arquivos, e ainda é usado certamente como um navegador de arquivos.

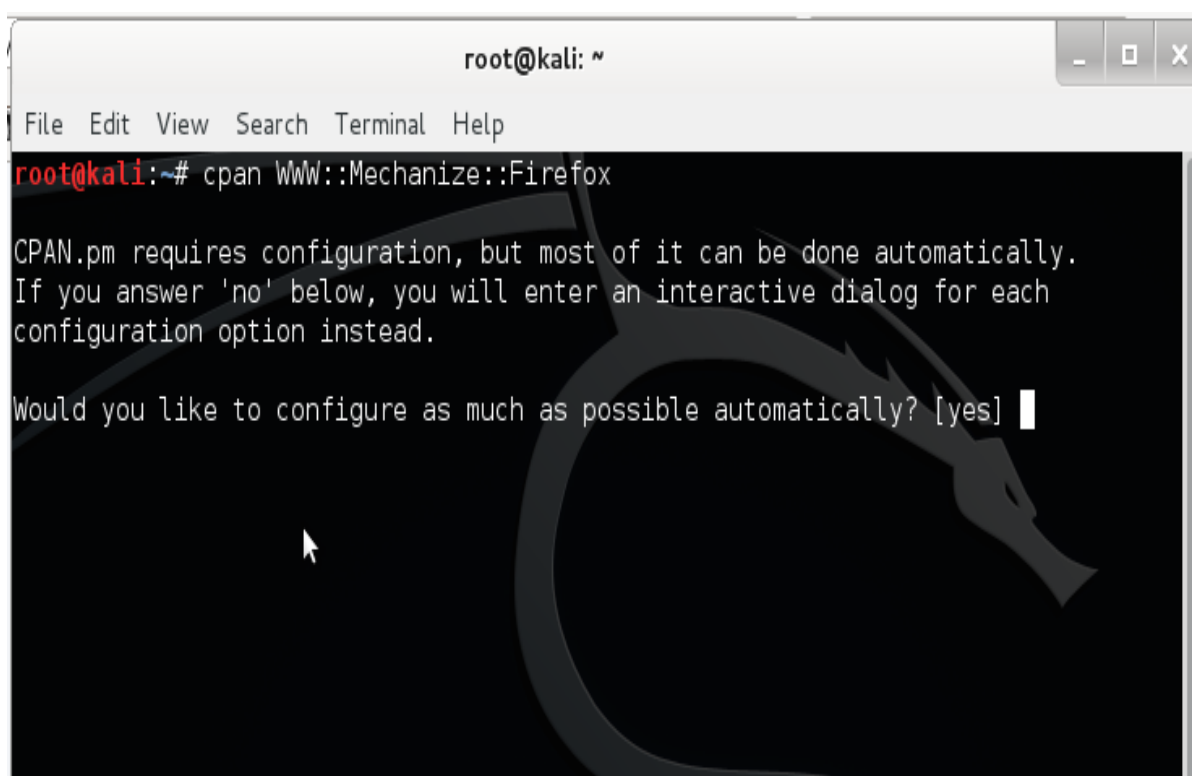



Figura 44: Instalando a biblioteca Mechanize de Firefox no sistema Kali Linux via terminal.
Fonte: Próprio autor.

Figura 45**:** Instalando o cpan MozRepel e cpan MozRepl::RemoteObject no sistema Kali Linux via terminal.

Fonte: Próprio autor.

Figura 46: *Debug* do código sistema *Information* pelo terminal.

Fonte: Próprio autor.

Figura 47: Debugando em tempo real o Sistema *Information* pelo terminal. (Autoria própria).
Fonte: Próprio autor.

### 7.13. **Mapeando com o Google Earth.**

O *Google Earth* é um *software* de computador desenvolvido e distribuído pela empresa *Google* cuja função é apresentar um modelo tridimensional do globo terrestre, construído a partir de mosaico de imagens de satélites obtidas de fontes diversas, imagens aéreas (fotografadas de aeronaves) e GIS 3D. Desta forma, o programa pode ser usado simplesmente com um gerador de mapas bidimensionais e imagens de satélite ou como um simulador das diversas paisagens presentes no Planeta Terra. Assim, possibilita identificar lugares, construções, cidades, paisagens, dentre outros elementos (GOOGLE, 2009).

Para demonstrar os resultados, em formato bidimensional foram feitas pesquisas de acordo com latitude e longitude dos dados obtidos pelo sistema *Information*.

Figura 48: Tela Inicial Google Earth.
Fonte: Google Earth, 2017.

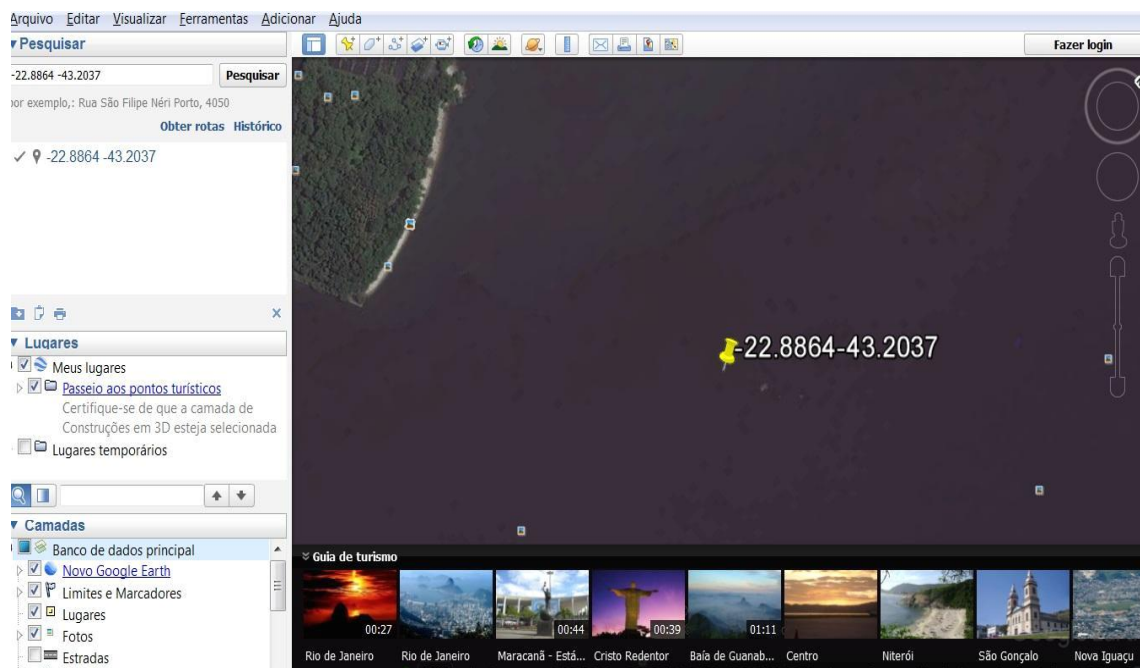



Figura 49: Latitude e Longitude do servidor do site Globo.
Fonte: Google Earth, 2017.

### 7.14. Repositório de código do GitLab.

*O GitLab* é um repositório *Git*, com base em nuvem e sistema de controle de versão usado por milhares de organizações em todo o mundo. É escrito em *Ruby*, a *GitLab* incluindo uma série de recursos que permitem às equipes de desenvolvimento de *software* consolidar o código-fonte, rastrear e gerenciar as versões, aumentar a qualidade do código, implementar mudanças de código e acompanhar a evolução do *software* ao longo do tempo. Além disso, o *GitLab* um sistema totalmente funcional de integração e entrega continua (CI/CD) que pode criar, testar e implantar atualizações de *software* à medida que equipe produz um novo código. O apoio da funcionalidade CI/CD do *GitLab* é um registro privado para contêiner *Docker*, permitindo que as equipes agilizem as atualizações para implantações de produção que estão sendo executadas em uma arquitetura de *microservices*.(BITNAMI, 2017).

O sistema *Information* será armazenado em nuvem utilizando *GitLab*. Segue abaixo o passo-a-passo para criação da pasta até *upload* do Sistema de *Information* para *GitLab*.

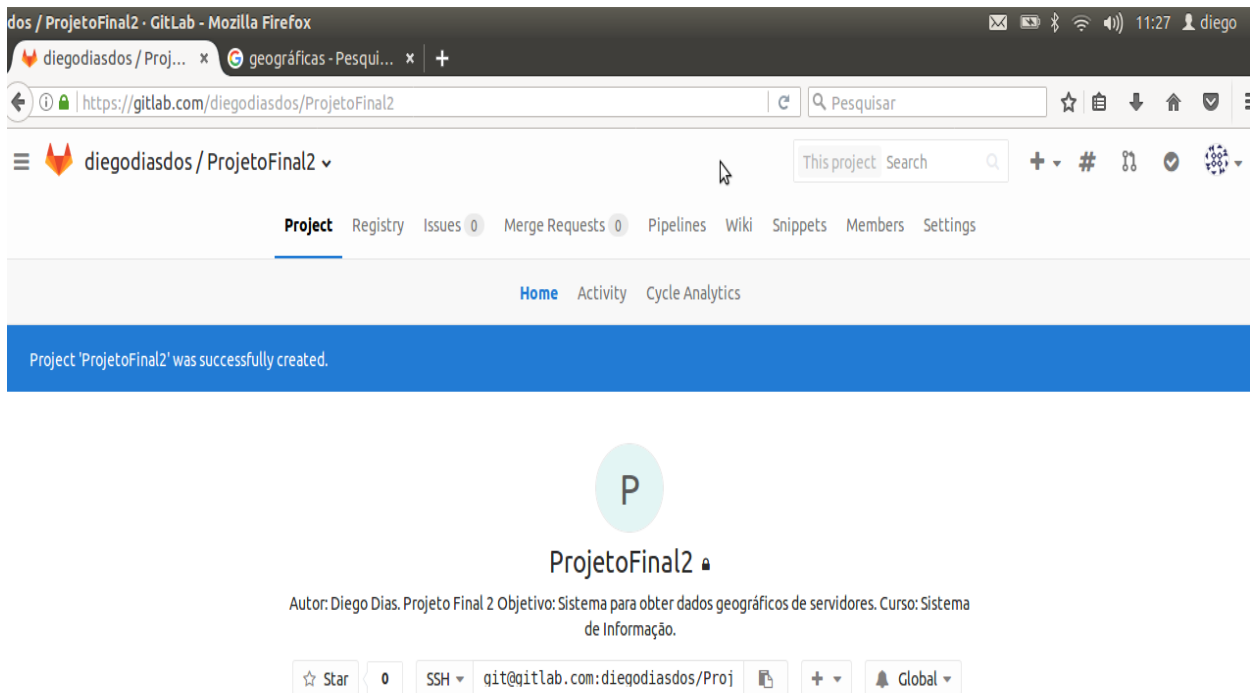



Figura 50: Criando pasta para sistema *Information*.
Fonte: Próprio autor.

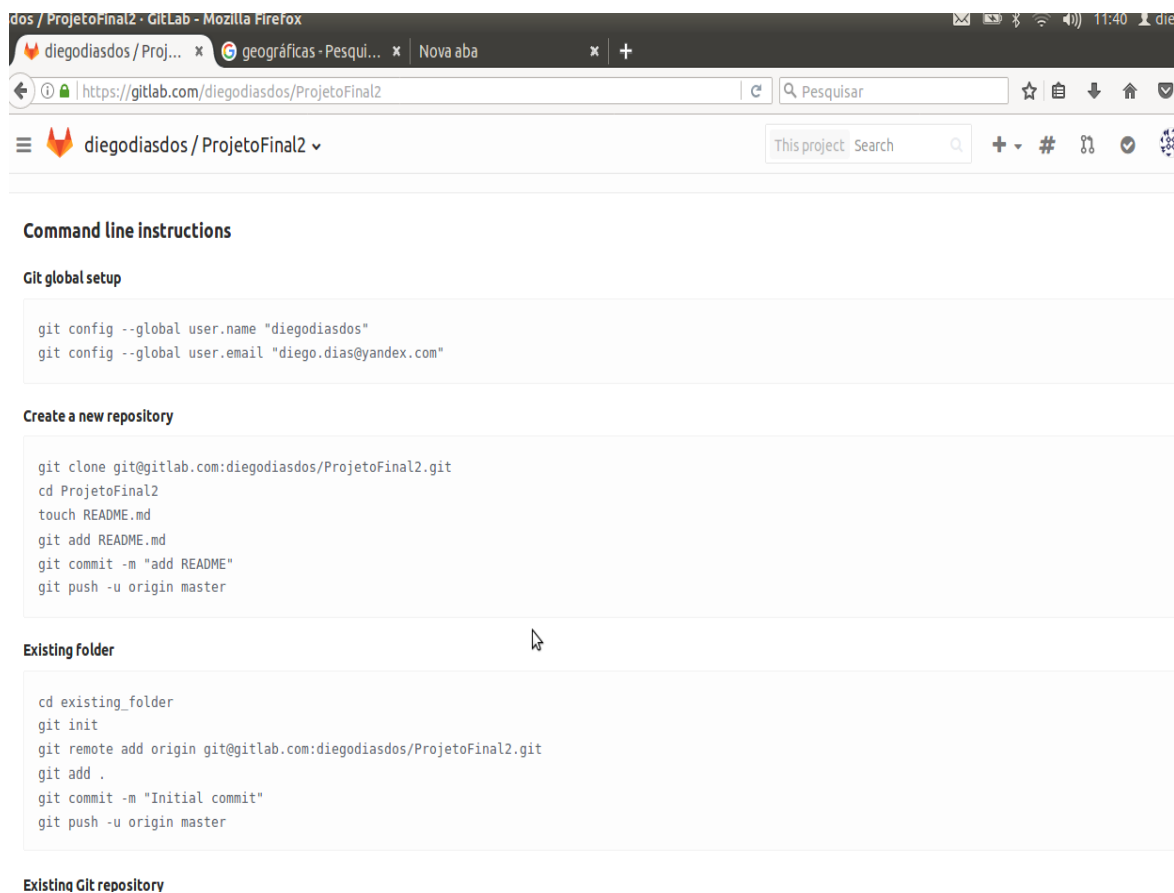



Figura 51: Comandos de Instruções para *GitLab*.
Fonte: Próprio autor.

```
diego@diego-Aspire-ES1-511: ~/Área de Trabalho
diego@diego-Aspire-ES1-511:~/Área de Trabalho$ git clone git@gitlab.com:diegodia
sdos/ProjetoFinal2.git
Cloning into 'ProjetoFinal2'...
warning: You appear to have cloned an empty repository.
diego@diego-Aspire-ES1-511:~/Área de Trabalho$
```

Figura 52: Clonando a pasta ProjetoFinal2.
Fonte: Próprio autor.

```
diego@diego-Aspire-ES1-511: ~/Área de Trabalho/ProjetoFinal2
diego@diego-Aspire-ES1-511:~/Área de Trabalho$ cd ProjetoFinal2/
diego@diego-Aspire-ES1-511:~/Área de Trabalho/ProjetoFinal2$ touch README.md
diego@diego-Aspire-ES1-511:~/Área de Trabalho/ProjetoFinal2$ git add README.md
diego@diego-Aspire-ES1-511:~/Área de Trabalho/ProjetoFinal2$ git commit -m "add
README"
[master (root-commit) 13b185d] add README
 0 files changed
 create mode 100644 README.md
```

Figura 53: Entrando na pasta ProjetoFinal2 e criando arquivo READ.md e depois adicionando no GitLab.
Fonte: Próprio autor.

```
diego@diego-Aspire-ES1-511:~/Área de Trabalho/ProjetoFinal2$ git push -u origin
master
Counting objects: 3, done.
Writing objects: 100% (3/3), 217 bytes, done.
Total 3 (delta 0), reused 0 (delta 0)
To git@gitlab.com:diegodiasdos/ProjetoFinal2.git
 * [new branch]      master -> master
Branch master set up to track remote branch master from origin.
```

Figura 54: Confirmando Upload do arquivo para GitLab.
Fonte: Próprio autor.

```
diego@diego-Aspire-ES1-511:~/Área de Trabalho/ProjetoFinal2$ cd
diego@diego-Aspire-ES1-511:~$ cd Área\ de\ Trabalho/
diego@diego-Aspire-ES1-511:~/Área de Trabalho$ mv Information.pl ProjetoFinal2/
diego@diego-Aspire-ES1-511:~/Área de Trabalho$ cd ProjetoFinal2/
diego@diego-Aspire-ES1-511:~/Área de Trabalho/ProjetoFinal2$ ls
Information.pl  README.md
diego@diego-Aspire-ES1-511:~/Área de Trabalho/ProjetoFinal2$ git add Information
.pl
diego@diego-Aspire-ES1-511:~/Área de Trabalho/ProjetoFinal2$ git commit -m " Inf
ormation"
[master 894bc2b]  Information
 1 file changed, 66 insertions(+)
 create mode 100644 Information.pl
diego@diego-Aspire-ES1-511:~/Área de Trabalho/ProjetoFinal2$
```

Figura 55: Movendo o sistema *Information* para pasta e carregando para nuvem do GitLab.
Fonte: Próprio autor.

Figura 56: O código do sistema *Information* armazenado na nuvem do Gitlab.
Fonte: Próprio autor.

## 8. CONCLUSÃO

Conclui-se que as empresas vêm buscando fazer vários testes em sistemas além de treinamentos com os funcionários, uma vez que as informações são muito importantes para qualquer organização, além do valor financeiro, que ficou claro, depois dos ataques cibernéticos  mundial que atingiram várias empresas inclusive órgãos do governo em vários países. Diante disso, este projeto objetivou demonstrar como é possível fazer o recolhimento de informações de empresa demonstrando suas falhas humanas e defeitos em sistemas de informações. Além de incluir uso das moedas *Bitcoins* utilizada pelos *hackers* para receber pagamentos de suas vítimas, diante dos ataques cibernéticos através de códigos maliciosos.

O projeto adicionou a computação forense em diferentes etapas que envolvem coleta, extração, análise, apresentação, dos dados dos alvos. Vale ressaltar a importância do mapa mental para gestão de informações e para o entendimento, bem como para solução de problemas, dentro da área de segurança da informação. Além disso, foi usada uma metodologia *Hacking* de Entrada Zero que demonstra o passo a passo em que *hacker* ético ou profissional de segurança de informação, deve fazer para descobrir falhas nos sistemas operacionais e falhas em sistemas *webs, e também o* descuido das pessoas que são manipuladas pela técnica de Engenharia Social.

Para desenvolver a tarefa de *hacking* ético e segurança da informação foi criado um relatório através sistema *Oracle Apex* que demonstra as falhas de sistemas registradas dentro da empresa de acordo com sua tecnologia, inclusive de sistemas de terceiros. Foram abordado o passo-a-passo das metodologias (ZEH) dentre elas o Reconhecimento(*Reconnaissace*) e a outra a Digitalização (*Scanning*), no processo de Reconhecimento foi utilizado *softwares* que estão inclusos no sistema operacional *Kali Linux* a primeira foi *httrack* que é utilizado

para clonar sites e trabalhar de forma *off-line* com código; o outro sistema é *theharvester* que permite o *Hacker* ético ou profissional de segurança de informação obter contas de *e-mails* dos usuários e *hostnames*/subdomínios através da URL de órgãos ou empresas através de fontes públicas de motores de busca como Google e servidores de chaves PGP(*Pretty Good Privacy*) dos alvos. Também foi incluído as técnicas de *Google Hacking* que serve para recolher informações através do *Google*, além de *Google Dorks* que mostra as falhas em sistemas através de busca no próprio *Google*. A Engenharia Social é uma técnica que permite que *Hackers* e profissionais de segurança da informação usem para induzirem as vítimas a fazerem algo que as mesmas não queiram através psicologia e fisiologia e tecnologia. Seguindo cronograma do projeto o sistema *Information* foi desenvolvido de com área de Engenharia de Software adotando a linguagem de modelagem unificada para construção do sistema e também foi incluído a metodologia *Scrum* através do software *Taiga* para acompanhar os processos do projeto. O sistema *Information* faz parte da etapa da digitalização da metodologia (ZEH), para recolher informações geográficas dos servidores de empresas a partir de URL "*Uniform Resource Locator*" ou protocolo *internet*, a tecnologia utilizada foi linguagem de programação *Perl* e biblioteca *CPAN*, além do link (ip-api.com) para buscar dados geográficos. O sistema foi testado através do terminal do *Kali Linux* para verificar os bugs e disponibilizado na nuvem na plataforma do *GitLab* com objetivo de armazenamento. E para se ter visão bidimensional dos dados geográficos recolhidos através do sistema *Information* dos servidores, foi utilizado o *Google Earth* que permite uma visão melhor dos locais de onde está sendo feito o recolhimento de informações.

O seguinte projeto também tem como objetivo um estudo para cibersegurança tendo como apoio softwares para proteger dados, que permite a cibersegurança em redes, exemplo disso são os servidores do *Ubuntu Server* que

faz uso de *Zabbix* o software que permite monitoramento da rede em todo os equipamentos que estão conectados nas redes, além de uma máquina virtual *Qemu* que permite utilizar sistema operacionais como *Tails* que permite os dados serem criptografados, além de utilizar software que permite navegar na internet de forma anônimo com endereços de outros países conhecido como *Tor* incluído com buscador *DuckDuckGo* que não coleta informações dos usuários que utiliza-se.

Para obter mais segurança dos dados principalmente na troca de e-mails foi acrescentado a *ProtonMail* que permite trocar mensagens e arquivos de forma criptografados através das redes. A Engenharia Social foi mencionada como uma forma de identificar técnicas *phishing* aplicado pelos *crackers* com fontes respeitáveis para obter dados das vítimas. Além disso, uso de redes *VPNS* para conexões com os servidores de forma criptografada permitindo que seus dados não sejam roubados ou tenha influência de invasão de privacidade. Com objetivo de influenciar projetos futuros, seria interessante uso de *APIS* com localização em tempo real para que o profissional de segurança possa saber a localização de usuários de aparelho móveis. Portanto, o projeto demonstrou como uma organização pode fazer uma perícia em sistemas a fim de encontrar falhas, tendo como suporte computação forense, além de capacitar os funcionários para protege-se de técnicas de Engenharia Social. E, de demonstrar construção de sistemas para recolhimento de informações, seguindo conceitos da Engenharia de *Software* com linguagem de modelagem unificada. Enfim, enfatizar o uso de *softwares* que podem dar mais segurança aos sistemas conectados em redes.

## REFERÊNCIAS

AGUIAR, V.M. (Org). **Software livre, cultura hacker e o ecossistema da colaboração**. - São Paulo: Momento Editorial, 2009.

ALCÂNTARA, B. T. **Brasil e Ciberterrorismo: desafios para o Rio 2016**. *International Conference on Forensic Computer Science* (ICOFCS). 2015, Brasília. Disponível em: <http://www.icofcs.org/2015/ICoFCS-2015-011.pdf> Acesso em: 18 mar. 2017.

ÂNGELO, F. K. Brasil lidera ranking mundial de hackers e crimes virtuais. **Folha de São Paulo**, 2002 http://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml> Acesso em 13 mar. 2017.

BALSAMIQ. Which version of Balsamiq is right for me? 2017. Disponível em: < https://balsamiq.com/products/> Acesso em: 26 de agosto de 2017.

BITNAMI. ***GitLab CE***. 2017. Disponível em: < https://bitnami.com/stack/gitlab > Acesso em:28 de agosto de 2017.

BISHOP FOX. GHDB Reborn Dictionaries - Exploit-DB. 2017. Disponível em: <https://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/> Acesso em: 26 de agosto de 2017.

CÂMARA, G; DAVIS, C. Por que geoprocessamento? In: CÂMARA, G; et al. (Org.) **Introdução à Ciência da Geoinformação**. São José dos Campos: INPE, 2001. p. 1-5. Disponível em: <http://www.dpi.inpe.br/gilberto/livro/introd/cap1-introducao.pdf> Acesso em: 13 mar. 2017.

CÂMARA, G; DAVIS, C. Por que geoprocessamento? In: CÂMARA, G; et al. (Org.) **Introdução à Ciência da Geoinformação**. São José dos Campos: INPE, 2001. p. 1-5. Disponível em: <http://www.dpi.inpe.br/gilberto/livro/introd/cap1-introducao.pdf> Acesso em: 13 mar. 2017.

CASTELLS, M. A galáxia da Internet. Rio de Janeiro: Jorge Zahar, 2003.

CELUPPI, Raphael. **Implantação do Zabbix para monitoramento de infraestrutura**. Trabalho de Conclusão do Curso de Especialização em Redes e Segurança de Sistemas. Curitiba, 2009. Disponível em: < https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Raphael%20Celuppi%20-%20Artigo.pdf> Acesso em: 26 de agosto de 2017.

CERT. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet**. Códigos maliciosos (Malware). 2017. Disponível em: <https://cartilha.cert.br/malware/> Acesso em: 26 julho de 2017.

DATASUS. Departamento de Informática do SUS. **Rio 2016: Tendência é de aumento de ciberataques a empresas e executivos**. 2016. Disponível em: <http://datasus.saude.gov.br/seguranca-da-informacao/noticias-seguranca-da-informacao/1016-rio-2016-tendencia-e-de-aumento-de-ciberataques-a-empresas-e-executivos> Acesso em: 18 mar. 2017.

DE SOUZA, P. F. C. **Perícia Forense Computacional**: procedimentos, ferramentas disponíveis e estudo de caso. Santa Maria: UFSM, 2015. 74p. (Trabalho de Conclusão de Curso) Curso Superior de Tecnologia em Redes de Computadores da Universidade Federal de Santa Maria, Santa Maria, 2015.

DE VASCONCELLOS, Marcio José Accioli. **A Internet e os hackers ataque e defesa**. Ed. Chantal. 460p. 2000.

DEBASTIANI, Carlos Alberto. **Definindo Escopo em Projetos de Software**. São Paulo: ed. Novatec 144p. 2015.

DISRUPTIVE LABS. **Host Discovery**. 2017. Disponível em: < http://disruptivelabs.in/art-of-packet-crafting-with-scapy/network_recon/host_discovery/index.html> Acesso em: 26 de agosto de 2017.

ECMA. *European Computer Manufacturers Association*. ***Standardizing Information and Communication Systems***. 1999. Disponível em:<https://www.ecma-international.org/publications/files/ECMA-ST-ARCH/ECMA-262,%203rd%20edition,%20December%201999.pdf> Acesso em: 26 de agosto de 2017.

El PAÍS. ***Los ciberataques a la OTAN crecieron un 60% en 2016***. Disponível em: <http://internacional.elpais.com/internacional/2017/03/13/actualidad/1489425600_231212.html> Acesso em: 18 mar. 2017

ENGEBRETSON, Patrick. **Introdução ao Hacking e aos Testes de Invasão**. São Paulo: ed. Novatec. 144p. 2014.

EXPLOIT-DB. Google Hacking Database (GHDB). 2017. Disponível em: < https://www.exploit-db.com/google-hacking-database/> Acesso em: 26 de agosto de 2017.

FRANCO, D. P. A Atuação do Perito Forense Computacional na Investigação de Crimes Cibernéticos. **Revista Cryotoid.** 2016. Disponível em: <https://cryptoid.com.br/banco-de-noticias/atuacao-do-perito-forense-computacional-na-investigacao-de-crimes-ciberneticos/> Acesso em: 13 mar. 2017.

GALIANO FILHO, Adilson. **Avaliação da Ferramenta Zabbix**. Trabalho de Conclusão do Curso de Especialização em Redes e Segurança de Sistemas.

Curitiba, 2010. Disponível em: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/Adilson%20Galiano%20-%20Artigo.pdf> Acesso em: 26 de agosto de 2017.

GARRETT, Filipe. Techtudo. **O que é VPN**? Saiba tudo sobre a rede virtual privada. 2014. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2015/11/o-que-e-vpn-saiba-tudo-sobre-rede-virtual-privada.html> https://googleblog.blogspot.com.br/2009/02/dive-into-new-google-earth.htmlGEOINFORMÁTICA. **Geoinformática.**2012. Disponível em:<http://geoinfoproyecto.blogspot.com> Acesso em: 23 de junho de 2017.

GOOGLE. **Mergulhe no novo Google Earth**. 2009. Disponível em:< https://googleblog.blogspot.com.br/2009/02/dive-into-new-google-earth.html> Acesso em: 26 de agosto de 2017.

GUNARTO, H. ***Ethical Issues in Cyberspace and IT Society***. Ritsumeikan Asia Pacific University. 2017. Disponível em: <http://www.apu.ac.jp/~gunarto/it1.pdf> Acesso em 13 mar. 2017.

IDN. Instituto da Defesa Nacional. **Estratégia da Informação e Segurança no Ciberespaço**. Lisboa: 2013. Disponível em: <http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf> Acesso em 14 mar. 2017.

INFOEUROPEFX. **Bitcoin price reached the historical level of 1857 dollars**. 2017. Disponível em: <https://www.infoeuropefx.com/bitcoin-price-reached-the-historical-level-of-1857-dollars/> Acesso em: 22 março de 2017.

KENT, K. et al. **Guide to integrating forensic techniques into incident response: recomendations of the National Institute of Standards and Technology. Special publication. Gaithersburg**: NIST, 2006.

LATTIMER, C. ***The Future of Geospatial Technologies in Securing Cyberspace.*** E- International Relations Students, 2013. Disponível em: <http://www.e-ir.info/2013/08/03/the-future-of-geospatial-technologies-in-securing-cyberspace/> Acesso em: 13 mar. 2017.

LÉVY, P. **Cibercultura**. Lisboa: Instituto Piaget, 1997.

LINUX DESCOMPLICADO. **Kali Linux: o sucessor do Backtrack**. 2017. Disponível em: https://www.linuxdescomplicado.com.br/2013/07/kali-linux-o-sucessor-do-backtrack.html> Acesso em: 26 de agosto de 2017.

MACEDO, Diego. **Firewall**. Disponível em: <https://www.diegomacedo.com.br/tag/firewall/> Acesso em: 27 de agosto de 2017.

MARQUES, R. **Fundamentos de Cartografia**: a Rede Geográfica. Departamento de Geociências. Universidade Federal da Paraíba, 2017. Disponível em: <http://www.geociencias.ufpb.br/leppan/disciplinas/lic/aula2.pdf> Acesso em: 13 mar. 2017.

MENDES, Douglas Rocha. **Redes de Computadores**: Teoria e Prática. São Paulo: ed. Novatec. 528p. 2007.

MOREIRA, Francisco et al. (2011) - *Landscape-wildfire interactions in southern Europe: Implications for landscape management*. ***Journal of environmental management*** 92 (10), 2389-2402

NICOLAU, L. A. **Sistema de informação geográfico-gerencial aplicado à gestão da qualidade na Segurança Pública.** Minas Gerais: UFLA, 2005. 80p. (Monografia) Departamento de Ciência da Computação da Universidade Federal de Lavras, Lavras, 2005.

NICOLAU, L. A. **Sistema de informação geográfico-gerencial aplicado à gestão da qualidade na Segurança Pública.** Minas Gerais: UFLA, 2005. 80p. (Monografia) Departamento de Ciência da Computação da Universidade Federal de Lavras, Lavras, 2005.

NIPP. ***National Infrastructure Protection Plan****: Partnering to enhance protection and resiliency*, DHS, 2009. Disponível em: <https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf> Acesso em 14 mar. 2017.

PIRES, Aécio. **Zabbix**: Uma ferramenta para Gerenciamento de ambientes de T.I. 2010. Disponível em: <https://pt.slideshare.net/aeciopires/zabbix-uma-ferramenta-para-gerenciamento-de-ambientes-de-ti> Acesso em: 26 de agosto de 2017.

READER, Ruth. **DuckDuckGo & Yummly team up so you can search food porn in private.** 2014. Disponível em: <https://venturebeat.com/2014/06/11/duckduckgo-yummly-team-up-so-you-can-search-food-porn-in-private/ > Acesso em: 27 de agosto de 2017.

RECESA. Rede de Capacitação e Extensão Tecnológica em Saneamento Ambiental. **Princípios básicos de geoprocessamento para seu uso em saneamento**. 2013. Disponível em: <http://nucase.desa.ufmg.br/wp-content/uploads/2013/07/principios-basicos-de-geoprocessamento.pdf> Acesso em: 13 mar. 2017.

REDES SEM FIO EM MALHA. **Arquitetura.** 2017. Disponível em: <https://www.gta.ufrj.br/grad/10_1/malha/arquitetura.html> Acesso em> 26 de março de 2017.

SANS, Securing the Human. Tradução: Michelini, Palheta Homero, 2014. O que

é um Antivírus? Disponível em: <https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201412_pt.pdf> Acesso em: 27 de agosto de 2017.

SEJA LIVRE.ORG. **Atualização do Tor, garante melhor anonimato na web**. 2017. Disponível em <http://sejalivre.org/atualizacao-do-tor-garante-melhor-anonimato-na-web> Acesso em: 26 de agosto de 2017.

SOUZA, A. G. Etapas do processo de computação forense: uma revisão. **Rev. Acta de Ciência e Saúde**. n. 5, v. 02, 99- 111p. 2016. Disponível em: <http://www2.ls.edu.br/actacs/index.php/ACTA/article/view/138> Acesso em: 13 mar. 2017.

SOUZA, Waslley. Oracle. Começando com Oracle APEX. 2015. Disponível em: <http://www.oracle.com/technetwork/pt/articles/apex/comecando-com-oracle-apex-2776847-ptb.html> Acesso em: 26 de agosto de 2017.

TAIGA. 2017. Disponível em: < https://taiga.io/> Acesso em: 26 de agosto de 2017.

TECMUNDO. **Tails: como transformar o seu PC em um dos mais seguros do mundo**. Disponível em < https://www.tecmundo.com.br/sistema-operacional/58213-tails-transformar-pc-seguros-mundo.htm> Acesso em: 27 de agosto de 2017.

TEIXEIRA, A.; et al. Qual a melhor definição de SIG, **Revista Fator GIS**, nº 11 Ano 3, Sagres Editora, Curitiba, 1995.

TERRAVIEW. **Conceitos Cartográficos**. 2011. Disponível em: <http://www.dpi.inpe.br/terraview/docs/pdf/ProjecaoCartografica.pdf> Acesso em: 13 mar. 2017.

TUDO PARA O SEU PC. **Códigos .bat (“Vírus”)**. 2017. Disponível em: <http://tudoopc.blogspot.com.br/2010/03/codigos.html> Acesso em: 26 de agosto de 2017.

UBUNTUPEDIA**, Sistema operacionais Ubuntu Server.** 2017. Disponível em:**<**http://ubuntupedia.info/index.php/Ubuntu_Server**>.** Acesso em: 11 julho 2017.

UNIXMEN. How To Install And Configure QEMU In Ubuntu. 2017. Disponível em <https://www.unixmen.com/how-to-install-and-configure-qemu-in-ubuntu/> Acesso em: 27 de agosto de 2017.

VAREJÃO, F. **Ética e Crimes Virtuais**. UFES, 2004. Disponível em: <http://www.inf.ufes.br/~fvarejao/cs/eticapeique.htm> Acesso em 13 mar. 2017.

YEN, Andy. **TED** – *Ideas Worth Spreading*.2015. Tradução: Gislene Kucker Arantes. Revisão: Ruy Lopes Pereira. Disponível em: <

https://www.brasil247.com/pt/247/revista_oasis/180814/Seu-e-mail-%C3%A9-privado-Se-voc%C3%AA-acha-que-sim-melhor-mudar-de-ideia.htm> Acesso em: 26 de agosto de 2017.